

COVARIANT ALGEBRA OF THE BINARY NONIC AND THE BINARY DECIMIC

REYNALD LERCIER AND MARC OLIVE

ABSTRACT. We give a minimal system of 476 generators (resp. 510 generators) for the algebra of $\mathrm{SL}_2(\mathbb{C})$ -covariant polynomials on binary forms of degree 9 (resp. degree 10). These results were only known as conjectures so far. The computations rely on Gordan's algorithm, and some new improvements.

1. INTRODUCTION

Invariant theory regularly comes up for discussion with numerous attempts to obtain new results. After the important Weyl's contribution [85] in the field of *representation theory*, many other reformulations have been made on the subject, as the ones of Dieudonné [31], Kung–Rota [57] or Howe [53, 54]. Most of them being of theoretic interest, the emergence of computer science revives interest in effective approaches, with the hope that new results could suddenly be reached. Besides, effective approaches also appear to have many important applications, as in continuum mechanics [69, 70, 9, 10], quantum informatics [61], recoupling theory [2, 3, 1, 4], cohomology of finite groups [5], computation of Galois groups [76, 42], cryptography [39, 40, 38], or combinatorics [72, 73].

Classical invariant theory¹, which is somewhat the cradle of invariant theory, was first initiated by Boole [11]. After this work, two different teams worked on the subject: an English one led by Cayley, Sylvester *et al.* [78, 20, 21] and a German one led by Clebsch, Gordan *et al.* [23, 47, 45, 46, 44, 43]. The first finiteness result, obtained by Gordan [43] in the case of $\mathrm{SL}(2, \mathbb{C})$ invariants of binary forms, was closely endowed with a constructive proof, namely Gordan's algorithm on binary forms [48, 86, 63]. As an application, Gordan and von Gall [82, 44, 84] obtained some non trivial finite *covariant basis* of binary forms: the ones of quintic [44, 48], sextic [44, 48], septic [44, 84] and octics [83]. All those computations were “hand made”, and up to nowadays, except computations made on octics [27, 6] or septimics [7], no any new results had been obtained in the topics of covariant basis of a single binary form.

Most of recent works on the subject [31, 57, 54, 28, 29, 30, 55, 77] make use of *algebraical geometry* tools, mainly developed by Hilbert himself [51]. One important step on this way is to obtain an homogeneous system of parameters (h.s.o.p), which gives degree upper-bounds on generators thanks to the *Hilbert series* of the invariant algebra. But calculating such a h.s.o.p is often difficult. Up to our knowledge, there is no general algorithm for this task, despite some recent attempts on that subject [49].

Nevertheless, in the case of binary forms, many theoretical results on h.s.o.p and Hilbert series have been obtained by Dixmier [32, 33, 34, 35]. In addition, Brouwer and Popoviciu [15, 14, 16, 17, 68] made important progress for nonics and decimics. For the first time, explicit h.s.o.p and minimal invariant basis were obtained for these spaces of binary forms.

We present in this article new results on covariant basis, which rely on mixed ideas coming from the classical algebraical geometry approach [31, 77, 14], some recent works made on *linear*

Date: September 30, 2015.

2010 Mathematics Subject Classification. 13C99, 14Q99.

Key words and phrases. Classical invariant theory; Covariants; Gordan's algorithm.

¹We can find an important literature on this subject made in the field of science sociology [41] or history of science [25, 26, 65].

Diophantine equation [22, 67] and a Gordan’s algorithm reformulation² [62]. We follow in a way Kung–Rota’s remark [57], “After Hilbert’s work, Gordan’s ideas were abandoned. However, Gordan’s method remains the most effective one”. We show with this approach that there exists a minimal covariant basis with 476 generators for the binary nonic (Theorem 24), respectively with 510 generators for the binary decimic (Theorem 25). We point out that those results have long been conjectured [13].

The paper is organized as follows. In Section 2, we give some mathematical backgrounds related to classical invariant theory of binary forms: definition of the invariant and covariant algebra, Cohen–Macaylayness property, Hilbert series, h.s.o.p. *etc.* In Section 3, we introduce Gordan ideals, which are the cornerstone of Gordan’s algorithm, presented subsequently in Section 3.3. Then, Section 4 focuses on some important improvements on Gordan’s algorithm and Section 5 gives details on calculation strategies that yield our new results. Finally, Section 6 presents all the computations and results obtained for the covariant algebra of binary nonics and decimics. For the sake of completeness, we explicit their minimal covariant basis in Appendix A and Appendix B.

2. MATHEMATICAL FRAMEWORK

2.1. Covariants of binary forms. The complex vector space of n -th degree binary forms, denoted S_n , is the space of homogeneous polynomials

$$\mathfrak{f}(\mathbf{x}) = a_0x^n + a_1x^{n-1}y + \dots + a_{n-1}xy^{n-1} + a_ny^n$$

with $\mathbf{x} = (x, y) \in \mathbb{C}^2$ and $a_i \in \mathbb{C}$. The natural $\mathrm{SL}_2(\mathbb{C})$ action on \mathbb{C}^2 induces a left action on S_n , given by

$$(g \cdot \mathfrak{f})(\mathbf{x}) := \mathfrak{f}(g^{-1} \cdot \mathbf{x}) \text{ for } g \in \mathrm{SL}_2(\mathbb{C}).$$

More generally, by a space V of binary forms, we mean a direct sum

$$V := \bigoplus_{i=0}^s S_{n_i}$$

where the action of $\mathrm{SL}_2(\mathbb{C})$ is diagonal.

The invariant algebra of V , denoted $\mathbf{Inv}(V)$, is the algebra $\mathbf{Inv}(V) := \mathbb{C}[V]^{\mathrm{SL}_2(\mathbb{C})}$. An important result, first established by Gordan [43], and then extended by Hilbert [51] to any linear reductive group, is the following.

Theorem 1. *For every space V of binary forms, the algebra $\mathbf{Inv}(V)$ is finitely generated, i.e. there exists a finite set $\{\mathbf{i}_1, \dots, \mathbf{i}_s\}$ in $\mathbf{Inv}(V)$, called a basis, such that*

$$\mathbf{Inv}(V) = \mathbb{C}[\mathbf{i}_1, \dots, \mathbf{i}_s].$$

The covariant algebra of a space V of binary forms, denoted $\mathbf{Cov}(V)$, is the invariant algebra

$$\mathbf{Cov}(V) := \mathbb{C}[V \oplus \mathbb{C}^2]^{\mathrm{SL}_2(\mathbb{C})}$$

with the action of $\mathrm{SL}_2(\mathbb{C})$ on $\mathbb{C}[V \oplus \mathbb{C}^2]$ defined by

$$(g \cdot p)(\mathfrak{f}, \mathbf{x}) := p(g^{-1} \cdot \mathfrak{f}, g^{-1} \cdot \mathbf{x}) \text{ for } g \in \mathrm{SL}_2(\mathbb{C}), p \in \mathbb{C}[V \oplus \mathbb{C}^2].$$

Similarly to $\mathbf{Inv}(V)$, the algebra $\mathbf{Cov}(V)$ is finitely generated.

There is a natural bi-gradation on the covariant algebra $\mathbf{Cov}(V)$,

- by the **degree** d , the polynomial degree in the coefficients of the space V ,
- and by the **order** m , the polynomial degree in the variables x, y .

²Note that Weyman [86] has also reformulated Gordan’s method in a modern way through algebraic geometry but, unfortunately, we were unable to extract from it an effective approach. There is also a preprint by Pasechnik [66] on this method.

We know an important upper-bound on the *order* of generators. For every integer n , we take λ to be the maximal integer such that $n = 2^\lambda + \nu$ and we define

$$\lambda_n := (\lambda - 1)2^\lambda + \nu(\lambda + 1) + 2. \quad (2.1)$$

Then we have this fact.

Lemma 2 ([48]). *For every space $V = \bigoplus_{i=0}^s S_{n_i}$ ($n_0 \leq \dots \leq n_s$) of binary forms, the covariant algebra $\mathbf{Cov}(V)$ is generated by covariants of maximum order λ_{n_s} .*

As a corollary, the covariant algebra $\mathbf{Cov}(S_9)$ (resp. $\mathbf{Cov}(S_{10})$) is generated by covariants of maximum order 22 (resp. 26).

We now focus on *minimal basis* of covariant algebras. Take a space V of binary forms and define $\mathbf{Cov}_{d,m}(V)$ to be the subspace of degree d and order m covariants. Now let

$$C_+ := \sum_{d+m>0} \mathbf{Cov}_{d,m}(V)$$

which is an ideal of the graded algebra $\mathbf{Cov}(V)$. For each (d, m) such that $d + m > 0$, let $\delta_{d,m}$ be the codimension of $(C_+^2)_{d,m}$ in $\mathbf{Cov}_{d,m}$. Since the algebra $\mathbf{Cov}(V)$ is of finite type, there exists an integer p such that $\delta_{d,m} = 0$ for $d + m \geq p$ and we can define the invariant number $n(V)$:

$$n(V) := \sum_{d,m} \delta_{d,m}.$$

Definition 3. A family $\{\mathbf{c}_1, \dots, \mathbf{c}_s\}$ is a *minimal basis* of $\mathbf{Cov}(V)$ if its image in the vector space C_+/C_+^2 is a basis. In that case, we have $s = n(V)$.

Remark 4. As pointed out by Dixmier–Lazard [36], a minimal basis is obtained by taking, for each couple (d, m) a complement basis of $(C_+^2)_{d,m}$ in $\mathbf{Cov}_{d,m}(V)$. There is a long history of an explicit determination of such a minimal basis for covariant algebras. We give in Table 1 some results (see [13] for a general overview). As far as we know, there is no way to obtain the invariant number $n(V)$ but to exhibit a minimal basis.

Algebra	$n(V)$	Explicit minimal basis
$\mathbf{Cov}(S_5)$	23	Gordan [43]
$\mathbf{Cov}(S_6)$	26	Gordan [43]
$\mathbf{Cov}(S_6 \oplus S_2)$	99	Von Gall [84]
$\mathbf{Cov}(S_7)$	147	Dixmier–Lazard [36], Bedratyuk [7]
$\mathbf{Cov}(S_8)$	69	Cröni [27], Bedratyuk [6] Popoviciu [68]
$\mathbf{Cov}(S_9)$	476	This paper
$\mathbf{Cov}(S_{10})$	510	This paper

TABLE 1. Minimal basis of covariant algebras

2.2. Cayley’s operator and transvectants. To calculate covariants, we make use of the *Cayley’s operator*, defined on a tensor product $S_n \otimes S_m$ (seen as a tensor product of complex analytic functions) by

$$\Omega_{\alpha\beta}(\mathbf{f}(\mathbf{x}_\alpha)\mathbf{g}(\mathbf{x}_\beta)) := \frac{\partial \mathbf{f}}{\partial x_\alpha} \frac{\partial \mathbf{g}}{\partial y_\beta} - \frac{\partial \mathbf{f}}{\partial y_\alpha} \frac{\partial \mathbf{g}}{\partial x_\beta}, \quad \mathbf{f} \in S_n, \quad \mathbf{g} \in S_m.$$

Definition 5. Given two binary forms $\mathbf{f} \in S_n$ and $\mathbf{g} \in S_m$, their *transvectant* of index $r \geq 0$, denoted $(\mathbf{f}, \mathbf{g})_r$, is defined to be

$$(\mathbf{f}, \mathbf{g})_r := \begin{cases} \frac{(n-r)!}{n!} \frac{(m-r)!}{m!} \mu \circ \Omega_{\alpha\beta}^r(\mathbf{f}(\mathbf{x}_\alpha)\mathbf{g}(\mathbf{x}_\beta)) & \text{if } 0 \leq r \leq \min(n, m), \\ 0 & \text{otherwise,} \end{cases}$$

where μ is a trace operator, $\mu(\mathfrak{h}(\mathbf{x}_\alpha, \mathbf{x}_\beta)) := \mathfrak{h}(\mathbf{x}, \mathbf{x})$.

Remark 6. There exists many other but equivalent definition of the transvectant, related to *group theory representation*. Indeed, $\mathrm{SL}(2, \mathbb{C})$ irreducible representations are given by spaces S_n of binary forms. By Clebsch–Gordan decomposition, we have

$$S_n \otimes S_m \simeq \bigoplus_{r=0}^{\min(n,m)} S_{n+m-2r},$$

and the unique projection (up to a scale factor) from $S_n \otimes S_m$ to S_{n+m-2r} is the transvectant.

2.3. Cohen–Macaulayness. We focus now on classical results issued from commutative algebra. We refer the interested reader to some general books [58, 87, 37, 18].

Let \mathcal{R} be a finitely generated graded \mathbb{C} -algebra,

$$\mathcal{R} = \bigoplus_{i \geq 0} \mathcal{R}_i, \quad \mathcal{R}_i \mathcal{R}_j \subset \mathcal{R}_{i+j}. \quad (2.2)$$

A finite family $\theta_1, \dots, \theta_s$ of free algebraic elements is a *homogeneous system of parameters* (h.s.o.p) if every element is homogeneous and if the algebra \mathcal{R} is a $\mathbb{C}[\theta_1, \dots, \theta_s]$ -module of finite type. The number s is nothing else than the *Krull dimension* [56] of \mathcal{R} . From the Noether normalization Lemma [58], a h.s.o.p always exists for a finitely generated ring. Nevertheless, this result is not constructive: up to our knowledge, there is no general algorithm to obtain a h.s.o.p, although some papers initiated the subject [49].

The algebra \mathcal{R} is said to be *Cohen–Macaulay* if it is a *free* $\mathbb{C}[\theta_1, \dots, \theta_s]$ -module of finite type. In that case, there exists elements η_1, \dots, η_r such that

$$\mathcal{R} = \eta_1 \mathbb{C}[\theta_1, \dots, \theta_s] \oplus \dots \oplus \eta_r \mathbb{C}[\theta_1, \dots, \theta_s]. \quad (2.3)$$

This direct sum is called the *Hironaka decomposition* of \mathcal{R} .

In invariant theory (for linear reductive group), an invariant algebra \mathcal{R} is always Cohen–Macaulay [52], especially $\mathbf{Inv}(V)$ is Cohen–Macaulay.

Take now \mathcal{M} to be a finitely generated graded \mathcal{R} -module and take again $\theta_1, \dots, \theta_s$ to be a h.s.o.p for \mathcal{R} . When the module \mathcal{M} is Cohen–Macaulay, we know that \mathcal{M} is a *free* $\mathbb{C}[\theta_1, \dots, \theta_s]$ -module. Thus there exists $\mathfrak{m}_1, \dots, \mathfrak{m}_p \in \mathcal{M}$ such that a Hironaka decomposition of \mathcal{M} is

$$\mathcal{M} = \mathfrak{m}_1 \mathbb{C}[\theta_1, \dots, \theta_s] \oplus \dots \oplus \mathfrak{m}_p \mathbb{C}[\theta_1, \dots, \theta_s]. \quad (2.4)$$

For a *covariant algebra* $\mathbf{Cov}(V)$, let us observe that for every integer $m > 0$, the space $\mathbf{Cov}_m(V)$ of m -th order covariants is a $\mathbf{Inv}(V)$ -module.

We have an important result due to Van Den Bergh [80, 81]. For every integer n , let us define

$$\sigma_n := \begin{cases} \frac{(n+1)^2}{4} & \text{if } n \text{ is odd,} \\ \frac{n(n+2)}{4} & \text{otherwise.} \end{cases}$$

Take now V to be the space of binary forms $\bigoplus_{i=0}^s S_{n_i}$ and let σ_V be $\sum_{i=0}^s \sigma_{n_i}$, we can state the following theorem.

Theorem 7. *For every integer $m < \sigma_V - 2$, the $\mathbf{Inv}(V)$ -module $\mathbf{Cov}_m(V)$ of m -th order covariants is Cohen–Macaulay.*

As a corollary, the $\mathbf{Inv}(S_9)$ -module $\mathbf{Cov}_m(S_9)$ is Cohen–Macaulay for every integer $m < 25$ and the $\mathbf{Inv}(S_{10})$ -module $\mathbf{Cov}_m(S_{10})$ is Cohen–Macaulay for every integer $m < 30$.

We now exhibit h.s.o.p. for $\mathbf{Inv}(S_9)$ and $\mathbf{Inv}(S_{10})$. Write first $\mathfrak{f} \in S_9$ and

$$\begin{aligned} \mathfrak{h}_1 &:= (\mathfrak{f}, \mathfrak{f})_8 \in S_2, & \mathfrak{h}_2 &:= (\mathfrak{f}, \mathfrak{f})_6 \in S_6, & \mathfrak{h}_3 &:= (\mathfrak{f}, \mathfrak{f})_4 \in S_{10}, & \mathfrak{h}_4 &:= (\mathfrak{f}, \mathfrak{f})_2 \in S_{14}, \\ \mathfrak{h}_5 &:= (\mathfrak{f}, \mathfrak{h}_2)_6 \in S_3, & \mathfrak{h}_6 &:= (\mathfrak{f}, \mathfrak{h}_5)_3 \in S_6, & \mathfrak{h}_7 &:= (\mathfrak{f}, \mathfrak{h}_5)_1 \in S_{10}, & \mathfrak{h}_8 &:= (\mathfrak{h}_2, \mathfrak{h}_2)_4 \in S_4, \\ \mathfrak{h}_9 &:= (\mathfrak{h}_5, \mathfrak{h}_5)_2 \in S_2, & \mathfrak{h}_{10} &:= (\mathfrak{h}_8, \mathfrak{h}_9)_0 \in S_6, & \mathfrak{h}_{11} &:= (\mathfrak{h}_8, \mathfrak{h}_9)_1 \in S_4. \end{aligned}$$

Proposition 8 ([34, 15]). *The algebra $\mathbf{Inv}(S_9)$ has a homogeneous system of parameters of degrees 4, 4, 8, 12, 14, 16 and 30 given by*

$$\begin{aligned} \mathfrak{p}_4 &:= (\mathfrak{h}_1, \mathfrak{h}_1)_2, & \mathfrak{q}_4 &:= (\mathfrak{h}_2, \mathfrak{h}_2)_6, & \mathfrak{p}_8 &:= (\mathfrak{h}_1^3, \mathfrak{h}_2)_6, & \mathfrak{p}_{12} &:= (\mathfrak{h}_1^5, \mathfrak{h}_3)_{10}, \\ \mathfrak{p}_{14} &:= (\mathfrak{h}_1^5, \mathfrak{h}_7)_{10}, & \mathfrak{p}_{16} &:= (\mathfrak{h}_1^7, \mathfrak{h}_4)_{14}, & \mathfrak{p}_{30} &:= ((\mathfrak{h}_{10}, \mathfrak{h}_{10})_4, \mathfrak{h}_{11})_4. \end{aligned}$$

The algebra $\mathbf{Inv}(S_9)$ has also homogeneous systems of parameters of degrees 4, 8, 10, 12, 12, 14, 16, degrees 4, 4, 10, 12, 14, 16, 24, degrees 4, 4, 8, 10, 12, 16, 42 and degrees 4, 4, 8, 10, 12, 14, 48.

Now let $\mathfrak{f} \in S_{10}$ and

$$\begin{aligned} \mathfrak{h}'_1 &:= (\mathfrak{f}, \mathfrak{f})_8 \in S_4, & \mathfrak{h}'_2 &:= (\mathfrak{f}, \mathfrak{h}'_1)_4 \in S_6, & \mathfrak{h}'_3 &:= (\mathfrak{f}, \mathfrak{f})_6 \in S_8, & \mathfrak{h}'_4 &:= (\mathfrak{h}'_3, \mathfrak{f})_8 \in S_2, \\ \mathfrak{h}'_5 &:= (\mathfrak{h}'_3, \mathfrak{h}'_3)_8 \in S_4, & \mathfrak{h}'_6 &:= (\mathfrak{h}'_2, \mathfrak{h}'_2)_4 \in S_4, & \mathfrak{h}'_7 &:= (\mathfrak{h}'_3, \mathfrak{h}'_5)_4 \in S_4. \end{aligned}$$

Proposition 9 ([14]). *The algebra $\mathbf{Inv}(S_{10})$ has a homogeneous system of parameters of degrees 2, 4, 6, 6, 8, 9, 10 and 14 given by*

$$\begin{aligned} \mathfrak{p}'_2 &:= (\mathfrak{f}, \mathfrak{f})_{10}, & \mathfrak{p}'_4 &:= (\mathfrak{h}'_1, \mathfrak{h}'_1)_4, & \mathfrak{p}'_6 &:= (\mathfrak{h}'_2, \mathfrak{h}'_2)_2, & \mathfrak{q}'_6 &:= (\mathfrak{h}'_4, \mathfrak{h}'_4)_2, \\ \mathfrak{p}'_8 &:= (\mathfrak{h}'_1, \mathfrak{h}'_6)_4, & \mathfrak{p}'_9 &:= ((\mathfrak{h}'_2, \mathfrak{h}'_1)_1, \mathfrak{h}'_1^2)_8, & \mathfrak{p}'_{10} &:= ((\mathfrak{h}'_2, \mathfrak{h}'_2)_2, \mathfrak{h}'_1^2)_8, \\ \mathfrak{p}'_{14} &:= ((\mathfrak{h}'_5, \mathfrak{h}'_5)_2, \mathfrak{h}'_7)_4 + ((\mathfrak{h}'_1, \mathfrak{h}'_1)_2^2, (\mathfrak{h}'_2, \mathfrak{h}'_2)_2)_8. \end{aligned}$$

2.4. Hilbert series and degree upper-bounds. Let $\mathcal{M} := \bigoplus_{i \geq 0} \mathcal{M}_i$ be a graded \mathcal{R} -module, its Hilbert series is defined to be

$$\mathcal{H}_{\mathcal{M}}(z) := \sum_{i \geq 0} \dim(\mathcal{M}_i) z^i.$$

A classical result states that the Hilbert series of a Cohen-Macaulay module with Hironaka decomposition given by (2.4) is

$$\mathcal{H}_{\mathcal{M}}(z) := \frac{z^{m_1} + \dots + z^{m_p}}{(1 - z^{d_1}) \dots (1 - z^{d_s})},$$

where m_i is the degree of \mathfrak{m}_i and d_j is the degree of θ_j .

If the family $\theta_1, \dots, \theta_s$ is a system of parameters, each subfamily $\theta_1, \dots, \theta_j$ ($j \leq s$) is a regular sequence and, writing

$$\overline{\mathcal{M}} := \mathcal{M} / (\theta_1 \mathcal{M} + \dots + \theta_j \mathcal{M}),$$

we have

$$\mathcal{H}_{\overline{\mathcal{M}}}(z) = (1 - z^{d_1}) \dots (1 - z^{d_j}) \mathcal{H}_{\mathcal{M}}(z). \quad (2.5)$$

In our case of interest, *i.e.* a covariant algebras of binary forms

$$\mathbf{Cov}(V) = \bigoplus_{d, m \geq 0} \mathbf{Cov}_{d, m}(V),$$

we make use of the *multi-graded* Hilbert series. Let $a_{d, m} := \dim(\mathbf{Cov}_{d, m}(V))$, we can define

$$\mathcal{H}_{\mathbf{Cov}(V)}(t, z) := \sum_{d, m \geq 0} a_{d, m} t^m z^d.$$

The Hilbert series of $\mathbf{Inv}(V)$ can be easily obtained from the *multi-graded* Hilbert series of $\mathbf{Cov}(V)$,

$$\mathcal{H}_{\mathbf{Inv}(V)}(z) = \mathcal{H}_{\mathbf{Cov}(V)}(0, z).$$

More generally, we can deduce the Hilbert series of the $\mathbf{Inv}(V)$ -module $\mathbf{Cov}_m(V)$ of m -th order covariants,

$$\mathcal{H}_{\mathbf{Cov}_m(V)}(z) = \sum_{d \geq 0} a_{d, m} z^d.$$

Finally, note that there exists many ways to compute such series *a priori* [79, 71, 60], especially Bedratyuk's developed a MAPLE package [8]. For a direct computation of a given $a_{d,m}$, we have this nice formula too.

Theorem 10 (Springer [71]). *The dimension of $\mathbf{Cov}_{d,m}(S_n)$ is equal to the $\lfloor (nd - m)/2 \rfloor$ -th coefficient of the power series expansion of*

$$\frac{(1 - q^n)(1 - q^{n+1}) \dots (1 - q^{n+d})}{(1 - q^2) \dots (1 - q^d)}.$$

When a h.s.o.p is known for a Cohen–Macaulay $\mathbf{Inv}(V)$ -module $\mathbf{Cov}_m(V)$, we directly deduce from its Hilbert series some upper-bounds on generator degrees.

Lemma 11. *The $\mathbf{Inv}(S_9)$ -module of m -th order covariant $\mathbf{Cov}_m(S_9)$ is generated by covariants of maximum degree d_m given in the following table, for $m \leq 22$:*

Ord. m	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
Max deg. d_m	66	61	64	63	62	63	64	63	62	65	64	63	62	63	64	63	62	63	64	63	62	63	62

Proof. For order 1 covariants, we know from Theorem 7 that $\mathcal{M} = \mathbf{Cov}_1(S_9)$ is a $\mathbf{Inv}(S_9)$ Cohen–Macaulay module. We also obtain by a direct computation $\mathcal{H}_{\mathcal{M}}(z) = a(z)/p(z)$ with

$$\begin{aligned} a(z) &= z^5 + 4z^7 + 10z^9 + \dots + z^{61}, \\ p(z) &= (1 - z^4)(1 - z^8)(1 - z^{10})(1 - z^{12})^2(1 - z^{14})(1 - z^{16}) \end{aligned}$$

where the numerator $p(z)$ corresponds to a h.s.o.p of $\mathbf{Inv}(S_9)$ given by Proposition 8. We deduce that the maximum degree of a generator is $d_1 = 61$. Similar calculations yield the results for the other orders m (note that for invariants, which are order 0 covariant, we make use of the $\mathbf{Inv}(V)$ Hironaka decomposition (2.3)). \square

Similarly, we have this table for S_{10} .

Lemma 12. *The $\mathbf{Inv}(S_{10})$ -module of m -th order covariant $\mathbf{Cov}_m(S_{10})$ is generated by covariants of maximum degree d_m given in the following table, for $m \leq 26$:*

Ord. m	0	2	4	6	8	10	12	14	16	18	20	22	24	26
Max deg. d_m	59	45	46	45	46	47	46	45	46	45	46	45	45	45

3. GORDAN'S ALGORITHM

Gordan's algorithm enables to compute a covariant basis for S_n , provided that a covariant basis is known for S_m , $m < n$. Roughly speaking, it consists in about $n/2$ iterations, each one giving a linear Diophantine system to solve. We put emphasis on the computational aspects of this method in this section. For more details, we refer the interested reader to the 19th century literature [43, 48], or to more modern works on that topic [86, 27, 62].

3.1. Relatively complete family and Gordan's ideal. For a finite family of covariants (not necessarily a basis) $A = \{f_1, \dots, f_p\} \subset \mathbf{Cov}(S_n)$, we define $\mathbf{Cov}(A)$ to be the closure of A under transvectant operations,

$$\mathfrak{h}_1, \mathfrak{h}_2 \in \mathbf{Cov}(A) \implies (\mathfrak{h}_1, \mathfrak{h}_2)_r \in \mathbf{Cov}(A), \quad \forall r \in \mathbb{N}.$$

Definition 13. Let $I \subset \mathbf{Cov}(S_n)$ be a homogeneous ideal, a family $A = \{f_1, \dots, f_p\} \subset \mathbf{Cov}(S_n)$ of homogeneous covariants is *relatively complete modulo I* if every homogeneous covariant $\mathfrak{h} \in \mathbf{Cov}(A)$ of degree d can be written

$$\mathfrak{h} = \mathbf{p}(f_1, \dots, f_p) + \mathfrak{h}_I \text{ with } \mathfrak{h}_I \in I,$$

where $\mathbf{p}(f_1, \dots, f_p)$ and \mathfrak{h}_I are degree d homogeneous covariants.

Remark 14. The notion of *relatively complete* family is weaker than the one of *generator set*. For instance, take $\mathbf{u} \in S_3$ and

$$\mathbf{h}_{2,2} := (\mathbf{u}, \mathbf{u})_2 \in S_2, \quad \mathbf{h}_{3,3} := (\mathbf{u}, \mathbf{h}_{2,2})_1 \in S_3, \quad \Delta := (\mathbf{h}_{2,2}, \mathbf{h}_{2,2})_2.$$

The family $A_1 = \{\mathbf{u}, \mathbf{h}_{2,2}, \mathbf{h}_{3,3}, \Delta\}$ is a covariant basis of $\mathbf{Cov}(A_1) = \mathbf{Cov}(S_3)$ and is thus a relatively complete family modulo $I = \{0\}$. Now, let $A_2 := \{\mathbf{h}_{2,2}, \Delta\}$. We have $\mathbf{Cov}(A_2) \subsetneq \mathbf{Cov}(S_3)$. Since A_2 is exactly the covariant basis of the quadratic form $\mathbf{h}_{2,2} \in S_2$, A_2 is a relatively complete family modulo $I = \{0\}$ but is not a covariant basis of $\mathbf{Cov}(S_3)$.

Definition 15 (Gordan's ideals). Let r be an integer. We define the Gordan ideal I_r to be the homogeneous ideal generated by the set of transvectants

$$\{(\mathbf{h}, (\mathbf{f}, \mathbf{f})_{r_1})_{r_2} : \mathbf{h} \in \mathbf{Cov}_{d,m}(S_n), \quad d, m \geq 0, \quad r_1 \geq r, \quad r, r_1, r_2 \in \mathbb{N}\}.$$

The ideal I_r is clearly a homogeneous ideal, as being generated by homogeneous elements. Moreover, we observe that:

- $I_r = \{0\}$ for all $r > n$;
- $I_{r+1} \subset I_r$ for all r ;
- $I_{2k-1} = I_{2k}$ for all $k \leq n/2$.

3.2. Linear Diophantine system. Take $A := \{\mathbf{f}_1, \dots, \mathbf{f}_p\}$, $B := \{\mathbf{g}_1, \dots, \mathbf{g}_q\}$ to be two finite covariant families of $\mathbf{Cov}(S_n)$ and consider the (infinite) family of transvectants

$$(\mathbf{U}, \mathbf{V})_r, \quad \text{with} \quad \mathbf{U} := \mathbf{f}_1^{\alpha_1} \dots \mathbf{f}_p^{\alpha_p}, \quad \mathbf{V} := \mathbf{g}_1^{\beta_1} \dots \mathbf{g}_q^{\beta_q}, \quad \alpha_i, \beta_j \in \mathbb{N}.$$

Define a_i (resp. b_j) to be the order of the covariant \mathbf{f}_i (resp. \mathbf{g}_j). Now, to each non-vanishing transvectant $(\mathbf{U}, \mathbf{V})_r$, we can associate an integer solution $\boldsymbol{\kappa} := ((\alpha_i), (\beta_i), u, v, r)$ of the linear Diophantine system

$$\mathcal{S}(A, B) : \quad \begin{cases} a_1 \alpha_1 + \dots + a_p \alpha_p &= u + r, \\ b_1 \beta_1 + \dots + b_q \beta_q &= v + r. \end{cases} \quad (3.1)$$

An integer solution $\boldsymbol{\kappa}$ of $\mathcal{S}(A, B)$ is *reducible* if we can decompose $\boldsymbol{\kappa}$ as a sum of non-trivial solutions. Conversely, there exists a finite family of *irreducible integer solutions* of the system $\mathcal{S}(A, B)$ (see [75, 74, 77] for details on linear Diophantine systems).

Now, to each integer solution $\boldsymbol{\kappa}$ of $\mathcal{S}(A, B)$, we can associate a well defined transvectant $(\mathbf{U}, \mathbf{V})_r$. Define $\boldsymbol{\kappa}^1, \dots, \boldsymbol{\kappa}^l$ to be the irreducible integer solutions of $\mathcal{S}(A, B)$ and $\boldsymbol{\tau}^i$ to be their associated transvectants. Let $\mathbf{f} \in S_n$, $\Delta \in \mathbf{Cov}(S_n)$ be an invariant, $k \geq 0$ be a given integer and $\mathbf{H}_{2k} := (\mathbf{f}, \mathbf{f})_{2k}$. Finally, let J_{2k+2} be either I_{2k+2} , or $I_{2k+2} + \langle \Delta \rangle$.

We have this important result.

Theorem 16 ([48]). *Suppose that A is relatively complete modulo I_{2k} and contains the binary form \mathbf{f} . Suppose also that B is relatively complete modulo J_{2k+2} and contains the covariant \mathbf{H}_{2k} . Then the family $C := \{\boldsymbol{\tau}^1, \dots, \boldsymbol{\tau}^l\}$ is relatively complete modulo J_{2k+2} and*

$$\mathbf{Cov}(C) = \mathbf{Cov}(A \cup B) = \mathbf{Cov}(S_n).$$

3.3. The algorithm. On input a degree n , Gordan's algorithm returns a basis for the covariant algebra $\mathbf{Cov}(S_n)$. All the details can be found in [48, 63].

First define $\mathbf{f} \in S_n$ to be a single binary form and $\mathbf{H}_{2k} := (\mathbf{f}, \mathbf{f})_{2k}$. The family $A_0 := \{\mathbf{f}\}$ is relatively complete modulo I_2 . This means that every covariant $\mathbf{h} \in \mathbf{Cov}(A_0)$ ($= \mathbf{Cov}(S_n)$) can be written as $\mathbf{h} = \mathbf{p}(\mathbf{f}) + \mathbf{h}_2$ with $\mathbf{h}_2 \in I_2$.

Take now the covariant $\mathbf{H}_2 := (\mathbf{f}, \mathbf{f})_2$ of order $2n - 4$.

- If $2n - 4 > n$, we take $B_0 := \{\mathbf{H}_2\}$ which is relatively complete modulo $J_4 := I_4$. Applying Theorem 16 leads us to a family $A_1 := C$ relatively complete modulo I_4 .

- If $2n - 4 = n$, we take $B_0 := \{H_2, \Delta\}$ which is relatively complete modulo $J_4 := I_4 + \langle \Delta \rangle$ with $\Delta := ((f, f)_{\frac{n}{2}}, f)_n$. In that case, by applying Theorem 16, we can take A_1 to be $C \cup \{\Delta\}$. A direct induction on the degree of the covariant shows that A_1 is relatively complete modulo I_4 .
- If $2n - 4 < n$, we suppose already known a covariant basis of S_{2n-4} . We then take B_0 to be this basis, which is finite and relatively complete modulo $J_4 := I_4$ (because relatively complete modulo $\{0\}$). We apply Theorem 16 to obtain $A_1 := C$.

Let now be given by induction a finite family A_{k-1} containing f and relatively complete modulo I_{2k} . We consider the covariant $H_{2k} := (f, f)_{2k}$.

- If H_{2k} is of order $m > n$, we take $B_{k-1} := \{H_{2k}\}$ which is relatively complete modulo $J_{2k+2} := I_{2k+2}$. By Theorem 16 we take $A_k := C$.
- If H_{2k} is of order $m = n$, we take $B_{k-1} := \{H_{2k}, \Delta\}$ which is relatively complete modulo $J_{2k+2} := I_{2k+2} + \langle \Delta \rangle$ with $\Delta := ((f, f)_{\frac{n}{2}}, f)_n$. In that case, by applying Theorem 16, we can take A_k to be $C \cup \{\Delta\}$. A direct induction on the degree of the covariant shows that A_k is relatively complete modulo I_{2k+2} .
- If H_{2k} is of order $m < n$, we suppose already known a covariant basis of S_m . We then take B_{k-1} to be this basis, which is relatively complete modulo $J_{2k+2} := I_{2k+2}$ (because relatively complete modulo $\{0\}$). We directly apply Theorem 16 to obtain $A_k := C$.

Finally, we have for $k = \lfloor n/2 \rfloor$ two cases, depending on n 's parity.

- If $n = 2q$, we know that the family A_{q-1} is relatively complete modulo I_{2q} . Furthermore the family B_{q-1} only contains the invariant $\Delta_q := \{f, f\}_{2q}$. Set $A_q := A_{q-1} \cup \{\Delta_q\}$.
- If $n = 2q + 1$, the family B_{q-1} contains the quadratic form $H_{2q} := \{f, f\}_{2q}$. We then know that the family B_{q-1} is given by the covariant H_{2q} and the invariant $\delta_q := (H_{2q}, H_{2q})_2$. By Theorem 16, set $A_q := C$.

In both cases, A_q is relatively complete modulo $I_{2q+2} = \{0\}$, it is thus a covariant basis.

4. IMPROVEMENTS OF GORDAN'S ALGORITHM

4.1. Shortened about relatively complete families. One important idea, that dates back to Gordan [43] and Von Gall [82] calculations, is to bypass the linear Diophantine system using relations between covariants and arguing directly modulo some Gordan ideal. This typically yields directly the reduced systems A_1 and A_2 , without using Theorem 16. Remind also that we always have $A_0 = \{f\}$, for $f \in S_n$ [48].

Lemma 17 ([44]). *For every integer $n \geq 4$, we have*

$$A_1 = \{f, H, T\}, \quad H := (f, f)_2, \quad T := (f, H)_1.$$

For every integer $n \geq 8$, we have

$$A_2 = \{f, H, T, K, (f, K)_1, (f, K)_2, (H, K)_1\}, \quad K := (f, f)_4.$$

4.2. Injective companion of a linear Diophantine system. We generalize to our situation the approach proposed by Clausen and Fortenbacher in the case of one equation [22], based on what they called the *injective companion* of a linear Diophantine equation.

Start from a system composed of two equations, written as

$$\begin{cases} \sum_{i \in I} a_i \left(\sum_{l=1}^{s(i)} \alpha_{il} \right) & = u + r, \\ \sum_{j \in J} b_j \left(\sum_{m=1}^{t(j)} \beta_{jm} \right) & = v + r, \end{cases} \quad (4.1)$$

with finite sets I, J of positive integers, mappings $s : I \rightarrow \mathbb{N}^*, t : J \rightarrow \mathbb{N}^*$ and natural integers $(a_i), (b_j), (\alpha_{il}), (\beta_{jm}), u, v$ and r . We now consider its injective companion

$$\begin{cases} \sum_{i \in I} a_i \alpha_i &= u + r, \\ \sum_{j \in J} b_j \beta_j &= v + r. \end{cases} \quad (4.2)$$

With a proof which is essentially the same as in [22], we obtain the next result.

Lemma 18. *$((\alpha_{il}), (\beta_{jm}), u, v, r)$ is a (minimal) solution of the linear Diophantine system (4.1) if and only if $((\alpha_i), (\beta_j), u, v, r)$ is a (minimal) solution of the injective companion (4.2), where*

$$\alpha_i := \sum_{l=1}^{s(i)} \alpha_{il} \text{ and } \beta_j := \sum_{m=1}^{t(j)} \beta_{jm}.$$

Remark 19. Given some $\alpha_i \geq 0$, the number of solutions $(\alpha_{il}) \geq 0$ of $\alpha_i = \alpha_{i1} + \alpha_{i2} + \dots + \alpha_{is(i)}$ is equal to the binomial coefficient $\binom{\alpha_i}{\alpha_i + s(i) - 1}$.

4.3. Relations on weighted monomials. Our aim is to take advantage of relations between covariants to ease some of the calculations in Gordan's algorithm. Note that the proofs of the results given below can be found in [63].

4.3.1. Commutative algebra. Let $x_1 > x_2 > \dots > x_p$ be indeterminates and $\mathcal{A} = \mathbb{C}[x_1, \dots, x_p]$ be a graded algebra of finite type. Consider also the lexicographic order on monomials of \mathcal{A} . We write $\mathbf{m}_1 \mid \mathbf{m}_2$ whenever the monomial \mathbf{m}_1 divides the monomial \mathbf{m}_2 .

Now, assume that there exist relations of those two different types.

Hypothesis 20. There exists a finite family $I \subset \{1, \dots, p-1\}$ and for each $i \in I$ a relation

$$(\mathcal{R}_i), \quad x_i^{a_i} = \sum_{k=0}^{a_i-1} x_i^k \mathbf{p}_k(x_{i+1}, \dots, x_p), \quad a_i \in \mathbb{N}^* \quad (4.3)$$

where \mathbf{p}_k is some polynomial. We write $\mathbf{m}_i := x_i^{a_i}$.

Hypothesis 21. There exists a finite family J and for each $j \in J$ a relation

$$(\mathcal{R}'_j), \quad x_{j_b}^{b_{j_b}} x_{j_c}^{c_{j_c}} = \mathbf{p}(x_{j_c+1}, \dots, x_p), \quad b_{j_b}, c_{j_c} \in \mathbb{N}^* \quad (4.4)$$

where $x_{j_b} > x_{j_c}$ and \mathbf{p} is some polynomial. We write $\mathbf{m}'_j := x_{j_b}^{b_{j_b}} x_{j_c}^{c_{j_c}}$.

Lemma 22. *Under Hypothesis 20 and Hypothesis 21, the algebra \mathcal{A} is generated by the family of monomials \mathbf{m} such that*

$$\mathbf{m}_i \nmid \mathbf{m}, \quad \mathbf{m}'_j \nmid \mathbf{m}, \quad \forall i \in I, \quad \forall j \in J.$$

4.3.2. Application to Gordan's algorithm. Gordan's algorithm deals with families A_0, B_0, \dots (see Section 3.3). Consider the case where the family B_{k-1} is the covariant basis of the binary form

$$H_{2k} = (f, f)_{2k} \in S_{2n-4k}.$$

H_{2k} is of order $2n - 4k < n$ and we suppose known its covariant basis. As in Theorem 16, write $\Delta \in \mathbf{Cov}(S_n)$ to be an invariant and $J_{2k+2} := I_{2k+2}$ or $J_{2k+2} := I_{2k+2} + \langle \Delta \rangle$. Write $A := A_{k-1}$, $B := B_{k-1}$ and note C to be the finite family of transvectants $(U, V)_r$ associated to irreducible solutions of the Diophantine system $\mathcal{S}(A, B)$ (cf. Equation (3.1)). Finally, suppose that Hypothesis 20 and Hypothesis 21 hold for the basis B of the algebra $\mathbf{Cov}(S_{2n-4k})$.

Theorem 23. *With the notations of Theorem 16, the subfamily \tilde{C} of C given by*

$$(U, \tilde{V})_r \in C, \quad \mathbf{m}_i \nmid \tilde{V}, \quad \mathbf{m}'_j \nmid \tilde{V}, \quad \forall i \in I, \quad \forall j \in J$$

is relatively complete modulo J_{2k+2} and

$$\mathbf{Cov}(\tilde{C}) = \mathbf{Cov}(A \cup B) = \mathbf{Cov}(S_n).$$

- (1) $\mathcal{G}_1 \leftarrow \{f\}$
- (2) For $d = 2, \dots, d_{\max}$:
 - (a) $\mathcal{G}_d \leftarrow \{\}$
 - (b) For each $H = \prod_{h \in \mathcal{G}_i} h$ s.t. $\deg H = d$:
 - If $H \notin \langle \mathcal{G}_d \rangle$ then $\mathcal{G}_d \leftarrow \mathcal{G}_d \cup \{H\}$
 where $\langle \mathcal{G}_d \rangle$ is the algebra generated by \mathcal{G}_d .
 - (c) $\Pi_{d-1} = \{H \mid H = \prod_{h \in \mathcal{G}_i} h \text{ and } \deg H = d-1\}$
 $h \in \mathcal{G}_i, \text{ ord } h \neq 0, \deg h \geq 2$
 - (d) For each $\mathbf{F} \in \Pi_{d-1}$, and each possible level r :
 - If $(\mathbf{F}, f)_r \notin \langle \mathcal{G}_d \rangle$ then $\mathcal{G}_d \leftarrow \mathcal{G}_d \cup \{(\mathbf{F}, f)_r\}$

FIGURE 1. Olver's algorithm

5. COMPUTATIONAL ASPECTS

5.1. Reformulating Theorem 16. The most computationally intensive steps of Gordan's algorithm are the ones which make use of Theorem 16 in order to obtain the families A_k . If Lemma 17 yields A_1, A_2 when $n \geq 8$ and if there exists a similar result for A_k when $2k \leq n/2$ (or equivalently when the order of $(f, f)_{2k}$ is greater or equal to n), we have in the remaining cases to solve a linear Diophantine system.

It turns out that using its injective companion as explained in Section 4.2 enables to find its minimal solutions, even if their number is very large (at least in degree 9 and 10, see Section 6 for details). Now, the covariants τ^l of family C in Theorem 16 associated to most of these solutions have large degrees and orders. Writing them as a polynomial is simply hopeless.

We solve this first issue as in [59]. In Gordan's algorithm, covariants result from transvectants of products of covariants, each one also recursively defined by transvectants. We thus represent them by the sequence of transvectants that must be done to obtain them. We do not have anymore their polynomial expressions, but we can still evaluate them on a binary form. In other words, a covariant is represented by an evaluation program. Note that it is immediate to determine the degree and the order of a covariant from the sequence of operations coded in an evaluation program.

Another difficulty is that taking for the family A_k all the corresponding transvectants τ^l 's yield huge computations in the following steps of Gordan's algorithm. To avoid this, we substitute to the family A_k a family A'_k which spans A_k . The purpose is to have A'_k much smaller than A_k (typically, few hundred of covariants instead of billions in our cases of interest). Incidentally, A'_k contains the binary form $f \in S_n$ and is still relatively complete modulo I_{2k+2} .

To define the family A'_k , we start from an algorithm³ published by Olver [64, p. 144] that aims at computing a basis for the sub-algebra of $\mathbf{Cov}(S_n)$ defined by generators of degree upper-bounded by some constant d_{\max} . Usually, as a preamble to Gordan's algorithm, it is good practice to run this algorithm for some d_{\max} chosen large enough to obtain a good candidate minimal basis $\mathcal{G} = \cup_{d \leq d_{\max}} \mathcal{G}_d$ for $\mathbf{Cov}(S_n)$ (cf. Algorithm 1).

This done, we consider in turn all the couples (d, m) of degrees/orders in the family A_k , sorted as considering first the spaces $\mathbf{Cov}_{d,m}(S_n)$ of smallest dimension. For each (d, m) , we check using linear algebra, e.g. Algorithm 2 (cf. Section 5.4), that the dimension of the homogeneous space $\langle \mathcal{G} \rangle_{d,m}$ is exactly the one of $\mathbf{Cov}_{d,m}(S_n)$. The latter is given by Springer formula (cf. Theorem 10). So, we ensure that $\langle A_k \rangle_{d,m} \subset \mathbf{Cov}_{d,m}(S_n) = \langle \mathcal{G} \rangle_{d,m}$ for all the couples (d, m) , and thus that $A_k \subset \langle \mathcal{G} \rangle$. We can then define A'_k as the subset of \mathcal{G} that spans A_k , or more precisely,

$$A'_k := \{c \in \mathcal{G} \mid \exists \tau \in A_k \text{ with } \deg c \leq \deg \tau \text{ and } \text{ord } c \leq \text{ord } \tau\}. \quad (5.1)$$

³Note that Olver's algorithm has only a *running bound* as shown by [12].

Under this viewpoint, we may see Gordan's algorithm as a way of having upper-bounds to prove that the basis returned by Olver's algorithm is minimal.

We did not encounter the problem in our $\mathbf{Cov}(S_9)$ and $\mathbf{Cov}(S_{10})$ calculations, but it might be possible that Algorithm 2 does not terminate at all for some (d, m) . This could be either because the basis \mathcal{G} is incomplete, or simply because of unfortunate random draws in the algorithm. To avoid this, let us define the subset $(A_k)_{d,m}$ to be the degree d and order m covariants of A_k . We then suggest to stop Algorithm 2 after a timeout and then check if there exist transvectants τ in $(A_k)_{d,m}$ that can complete the basis of covariants constructed so far. We may perform this task as in Step (4) of this algorithm where we replace the covariant random draws at Step (4.a) by the enumeration of $(A_k)_{d,m}$. Of course, we have to enlarge the set defined in Equation (5.1) with these τ to define here A'_k .

Still, we stress that we are in trouble when, despite all that, $\langle A'_k \rangle_{d,m} \subsetneq \mathbf{Cov}_{d,m}(S_n)$, since we can not exclude that, again due to unfortunate random draws, this procedure wrongly detects that some evaluation of τ is in the associated projection of $\langle \mathcal{G} \rangle$, while the covariant τ itself is not in $\langle \mathcal{G} \rangle$. Missing such a τ might yield at the end of Gordan's algorithm a wrong basis for $\mathbf{Cov}(S_n)$. In such a very exceptional case, the best in our opinion is to restart from the beginning the whole computation with a better basis $\langle \mathcal{G} \rangle$, which means running Olver's algorithm with a largest d_{\max} .

Now, we can optimize all the computations using different techniques: a first one based on upper-bounds on degrees and orders, the second one based on computation reduction and the third one based on linear algebra.

5.2. Upper-bounds on degrees and orders. Now, several of the improvements stated in the paper come into play. We can first reduce some covariants of the family A_k using the relations that we may have calculated between covariants of B_{k-1} (see Theorem 23). Typically, assuming that we have ordered the covariants of B_{k-1} by some inequality relation $<$, if we have for some $C_1 > C_2$ a relation of the form

$$C_1^{e_1} \times C_2^{e_2} = \sum \prod_{C < C_2} C$$

then we have Hypothesis 21 and we can use Theorem 23. Thus we can discard minimal solutions that yield transvectants of the form

$$\left(\prod_{c_i \in A_{k-1}} c_i^{a_i}, C_1^{e_1} \times C_2^{e_2} \prod_{u_i \in B_{k-1}} u_i^{b_i} \right)_r.$$

This process often results in decreasing the number of couples (d, m) of degrees/orders in the family A_k .

We can further make use of upper-bounds known on the degree d and the order m of a basis. Especially, we know

- from Grace and Young [48], that the order m can be upper-bounded by Equation (2.1),
- from Van Den Bergh [80, 81] and the Cohen–Macaulayness property of some $\mathbf{Cov}_m(S_n)$ module (see Theorem 7), that for orders m of medium size, the degree d can be upper-bounded by the largest exponent that arises in the numerator of a rational expression of the Hilbert series of $\mathbf{Cov}_m(S_n)$, related to a given h.s.o.p of $\mathbf{Inv}(S_n)$.

The later upper-bounds are very spectacular in practice, see Lemma 11 or Lemma 12.

5.3. Reductions. We may remark that the computations can be done

- modulo a subfamily $\theta_1, \dots, \theta_j$ of a system of parameters for $\mathbf{Inv}(S_n)$,
- modulo a small prime p , typically $p = 65521$.

- (1) Draw $(1 + O(1)) \times \dim \mathbf{Cov}_{d,m}(S_n)$ random covariants (\mathbf{c}_i) in $\langle \mathcal{G} \rangle_{d,m}$.
- (2) Evaluate these \mathbf{c}_i at $\dim \mathbf{Cov}_{d,m}(S_n)/(k+1) + O(1)$ forms (f_j) chosen at random this yields a matrix $\mathbf{M} = (\mathbf{c}_i(f_j))_{i,j}$.
- (3) Compute the “parity-check” matrix \mathbf{M}^\top of \mathbf{M} .
(i.e. $\mathbf{c} \times \mathbf{M}^\top = \mathbf{0}$ if $\mathbf{c} = \mathbf{M} \times \mathbf{v}$ for some vector \mathbf{v})
- (4) While $\text{rank} \mathbf{M} < \dim \mathbf{Cov}_{d,m}(S_n)$,
 - (a) look for a $\mathbf{c} \in \langle \mathcal{G} \rangle_{d,m}$ s.t. $\mathbf{M}^\top \times (\mathbf{c}(f_j)) \neq 0$,
 - (b) update \mathbf{M}^\top .

FIGURE 2. Checking that a covariant family \mathcal{G} generates $\mathbf{Cov}_{d,m}(S_n)$

In both cases, if the images of the covariants under reduction are independent, then the covariants are independent. So, instead of checking that the dimension of some $\mathcal{M} = \mathbf{Cov}_{d,m}(S_n)$ satisfies Springer’s dimension over \mathbb{Q} or \mathbb{C} , it is enough to check that the dimension of $\mathcal{M}/(\theta_1\mathcal{M} + \dots + \theta_j\mathcal{M})$ is modulo p the one derived from the Hilbert series given by Equation (2.5).

5.4. Linear algebra. To check the dimensions of the numerous homogeneous spaces $\langle \mathcal{G} \rangle_{d,m}$ that arise in Gordan’s algorithm, we finally proceed as in the Las-Vegas type probabilistic Algorithm 2. It terminates with the correct answer, but its running time depends on random choices. Its main advantage is that it makes only one Gauss elimination.

It works as follows:

- in Step (1), we first chose at random slightly more than $D := \dim \mathbf{Cov}_{d,m}(S_n)$ covariants;
- we evaluate them in Step (2) at enough binary forms to obtain a matrix \mathbf{M} (remember that these covariants are given by an evaluation program);
- we compute in Step (3) by a Gauss elimination a basis for the dual of the vector space defined by \mathbf{M} , and incidentally we have the rank of \mathbf{M} (it is expected that this rank is close to D);
- in the Step (4) loop, we look for a covariant the evaluation vector of which is not orthogonal to \mathbf{M}^\top and when this is the case, update \mathbf{M}^\top (this can be done incrementally with complexity only $O(D^2)$).

In such a computation, we observe that it is relatively easy to find generators that span a subspace of $\mathbf{Cov}_{d,m}(S_n)$ with a dimension close to the awaited dimension D . Actually, most of the time is finally spend in Step (4.a) while looking for the very few additional generators needed to reach the dimension D . But this step is straightforward enough to be easily implemented and optimized in a program written at low level, in language C. Furthermore, it is highly parallelizable on a multi-core computer: give one covariant \mathbf{c} to each core, either while computing \mathbf{M} , or looking for a covariant \mathbf{c} s.t. $\mathbf{M}^\top \times (\mathbf{c}(f_j)) \neq 0$.

It may be worth to add that here “choosing at random covariants” simply means to first choose at random products of covariants in \mathcal{G} with the expected degree and a large enough order, and then to calculate a transvectant of suitable level. We just observe in practice that avoiding to take invariants as terms in these products improves significantly the chances of finding a new independent covariant in Step (4.a).

6. RESULTS

6.1. Covariant basis of binary nonics. We start from the possibly incomplete basis known for the algebra $\mathbf{Cov}(S_9)$. Such a basis have been already computed in the past, (see for instance [13]). We develop our own implementation of Olver’s algorithm and ran it with a large upper-bound d_{\max} , e.g. $d_{\max} = 30$. We retrieve a basis with 476 generators. A complete but somehow unappealing definition for these generators is in Appendix A. We give instead in Table 2 the number of generators for each degree and each order.

All in all, the calculations that follow enables us to prove this theorem.

Theorem 24. *The 476 covariants given in Appendix A define a minimal basis for the covariant algebra $\mathbf{Cov}(S_9)$.*

$d/o.$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	21	22	#	Cum	
1	—	—	—	—	—	—	—	—	—	1	—	—	—	—	—	—	—	—	—	—	—	—	1	1	
2	—	—	1	—	—	—	1	—	—	—	1	—	—	—	1	—	—	—	—	—	—	—	4	5	
3	—	—	—	1	—	1	—	1	—	2	—	1	—	1	—	1	—	1	—	—	1	—	10	15	
4	2	—	—	—	2	—	2	—	3	—	2	—	2	—	2	—	1	—	1	—	—	1	18	33	
5	—	1	—	3	—	4	—	4	—	3	—	4	—	2	—	3	—	—	—	1	—	—	25	58	
6	—	—	4	—	4	—	6	—	6	—	3	—	4	—	—	—	1	—	—	—	—	—	28	86	
7	—	4	—	7	—	8	—	7	—	6	—	1	—	1	—	—	—	—	—	—	—	—	34	120	
8	5	—	8	—	10	—	10	—	4	—	2	—	—	—	—	—	—	—	—	—	—	—	39	159	
9	—	9	—	14	—	10	—	7	—	1	—	—	—	—	—	—	—	—	—	—	—	—	41	200	
10	5	—	15	—	15	—	3	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	39	239	
11	—	17	—	16	—	7	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	41	280	
12	14	—	23	—	4	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	42	322	
13	—	25	—	10	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	36	358	
14	17	—	13	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	31	389	
15	—	26	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	27	416	
16	21	—	3	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	24	440	
17	—	7	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	7	447	
18	25	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	25	472	
19	—	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	1	473	
20	2	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	2	475	
21	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	475
22	1	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	1	476	
Tot	92	90	67	52	36	31	23	20	14	13	8	6	6	4	3	4	2	1	1	1	1	1	476		

TABLE 2. Minimal basis of $\mathbf{Cov}(S_9)$

6.1.1. *Gordan iterations.* We follow Section 3.3.

- We start from $A_0 = \{f\}$.
- Set $H := (f, f)_2$, we know from Lemma 17 that

$$A_1 = \{f, H, T\} \text{ with } T := (f, H)_1.$$

- The family A_2 is (similarly) given by

Cov.	f	$h_{10} := (f, f)_4$	$h_{14} := (f, f)_2$	$(f, h_{10})_2$	$(f, h_{10})_1$	$(f, h_{14})_1$	$(h_{10}, h_{14})_1$
Ord.	9	10	14	15	17	21	22
Deg.	1	2	2	3	3	3	4

We have now to compute with Theorem 16 the family A_3 , using the family A_2 .

- Let B_2 be the covariant basis of $c_3 := (f, f)_6 \in S_6$. As a classical result [48], such a basis is given by 26 covariants, and we only keep the family of $26 - 5 = 21$ covariants (see the next table).
- A_3 is then composed of transvectants of the type

$$\left(\prod_{h \in A_2} h^a, \prod_{C \in B_2} C^b \right)_r \quad (6.1)$$

We keep a finite number of them, those that come from minimal solutions of a linear Diophantine system. This is the difficult part (see Section 6.1.2).

- We take few additional transvectants with $c_2 = (f, f)_8 \in S_2$, and we finally obtain a covariant basis for $\mathbf{Cov}(S_9)$.

d/o	0	2	4	6	8	10	12	#	Cum
1	—	—	—	1	—	—	—	1	1
2	1	—	1	—	1	—	—	3	4
3	—	1	—	1	1	—	1	4	8
4	1	—	1	1	—	1	—	4	12
5	—	1	1	—	1	—	—	3	15
6	1	—	—	2	—	—	—	3	18
7	—	1	1	—	—	—	—	2	20
8	—	1	—	—	—	—	—	1	21
9	—	—	1	—	—	—	—	1	22
10	1	1	—	—	—	—	—	2	24
11	—	—	—	—	—	—	—	—	24
12	—	1	—	—	—	—	—	1	25
13	—	—	—	—	—	—	—	—	25
14	—	—	—	—	—	—	—	—	25
15	1	—	—	—	—	—	—	1	26
Tot	5	6	5	5	3	1	1	26	

6.1.2. *Linear integer system.* Taking the orders of covariants occurring in transvectants given by (6.1) lead to the following integer system $((a_i), (b_j), u, v, r \geq 0)$:

$$(\mathcal{S}) \begin{cases} 9a_1 + 10a_2 + 14a_3 + 15a_4 + 17a_5 + 21a_6 + 22a_7 & = u + r, \\ 2(b_1 + b_2 + b_3 + b_4 + b_5 + b_6) + 4(b_7 + b_8 + b_9 + b_{10} + b_{11}) + \\ 6(b_{12} + b_{13} + b_{14} + b_{15} + b_{16}) + 8(b_{17} + b_{18} + b_{19}) + 10b_{20} + 12b_{21} & = v + r. \end{cases}$$

There are numerous works on how to compute minimal solutions of linear integer systems [22, 24]. Further, there exist optimized and reliable implementations, typically NORMALIZ used in MACAULAY 2 [19], or 4Ti2 and especially, the so-called program HILBERT [50]. In our case, we have only 2 linear equations, HILBERT performs better than NORMALIZ. But the system for $\mathbf{Cov}(S_9)$ has so many minimal solutions that we had to abort calculations after several hours of computation.

Following Section 4.2, we regroup variables with same coefficients in (\mathcal{S}) , *i.e.* $\beta_1 = b_1 + b_2 + b_3 + b_4 + b_5 + b_6$, $\beta_2 = b_7 + b_8 + b_9 + b_{10} + b_{11}$, *etc.* and we consider the injective companion of (\mathcal{S}) ,

$$(\tilde{\mathcal{S}}) \begin{cases} 9a_1 + 10a_2 + 14a_3 + 15a_4 + 17a_5 + 21a_6 + 22a_7 & = u + r, \\ 2\beta_1 + 4\beta_2 + 6\beta_3 + 8\beta_4 + 10\beta_5 + 12\beta_6 & = v + r. \end{cases}$$

This time, the software HILBERT returned 7338 solutions in only 25 seconds on a laptop. From Remark 19, we finally found that the 7338 solutions of $(\tilde{\mathcal{S}})$ yield 58 525 823 minimal solutions of (\mathcal{S}) .

d/o	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	...
1	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	...
2	-	-	-	-	-	-	✓	-	-	-	✓	-	✓	-	-	...
3	-	-	-	✓	-	✓	-	✓	-	✓	-	✓	-	✓	-	...
4	-	-	-	-	✓	-	✓	-	✓	-	✓	-	✓	-	✓	...
5	-	✓	-	✓	-	✓	-	✓	-	✓	-	✓	-	✓	-	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	...
268	✓	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	...
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	...
502	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	...
506	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	...
510	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	-	...

TABLE 3. Couples (d, m) for the family A_3

These 58 525 823 minimal solutions yield transvectants that we can gather by degree d and order m . It covers 1836 couples (d, m) (*cf.* Table 3). For instance, the last row corresponds to the transvectant $(\mathfrak{c}_{15}^2, \mathbf{C}_{24,2}^{21})_{42}$ where \mathfrak{c}_{15} is the covariant of degree 3 and order 21 defined in Appendix A and $\mathbf{C}_{24,2}$ is the covariant of degree 12 and order 2 in the table of S_6 evaluated at \mathfrak{c}_3 (*cf.* Section 6.1.1) which lead to a covariant of degree 24 in \mathfrak{f} .

Following Section 5.1, we have now to compute the dimensions of these 1836 homogeneous spaces $\mathbf{Cov}_{d,m}(S_9)$. But Theorem 10 yields for instance $\dim \mathbf{Cov}_{501,0}(S_9) = 14\,510\,116\,319$, which is far too large to be checked.

6.1.3. *Degree and order upper-bounds.* Now, the upper-bounds of Section 5.2 help to simplify a lot the computations.

- Using Lemma 2, we can restrict to orders $m \leq 22$.
- Using Lemma 11, we have degree upper-bounds for every order $m \leq 22$.

Finally, $\mathbf{Cov}_{64,18}(S_9)$ is one of the largest case that remains. Now, $\dim \mathbf{Cov}_{64,18}(S_9) = 1\,576\,149$ is much smaller than $\dim \mathbf{Cov}_{501,0}(S_9)$, but it is obviously still too large for Algorithm 2.

6.1.4. *Relations.* Following Section 5.3, we looked for relations between covariants of B_2 , which is the covariant basis of S_6 . Let us order the covariants of B_2 first by degree then by order, invariants last,

$$C_{24,2} > C_{20,2} > C_{18,4} > C_{16,2} > \dots > C_{4,8} > C_{2,6} > C_{30,0} > C_{10,0} > C_{12,0} > C_{8,0} > C_{4,0}$$

(we write $C_{2d',m}$ for the covariant of degree d' in $\mathfrak{c}_3 \in S_6$ and order m , all being taken from the classical covariant basis of S_6 given for example in [48]).

We found 18 relations of the form

$$C_{d,m}^e = \sum \prod_{C < C_{d,m}} C$$

(where the power e goes from 2 for $C_{24,2}$ up to $e = 9$ for $C_{6,8}$) and for any $C_1 > C_2$ several hundred relations of the form

$$C_1^{e_1} \times C_2^{e_2} = \sum \prod_{C < C_2} C.$$

Thanks to the degree/order upper-bounds and the relations for B_2 , only 235 493 transvectants remain. It decreases the number of spaces $\mathbf{Cov}_{d,m}(S_9)$ to be tested to 633 (instead of 1836). The largest one is $\mathbf{Cov}_{60,14}(S_9)$, its dimension is about 2 times smaller than $\mathbf{Cov}_{66,18}(S_9)$,

$$\dim \mathbf{Cov}_{60,14}(S_9) = 872\,368,$$

but it is still slightly too large for Algorithm 2 (the complexity of which is at least cubic in this dimension).

6.1.5. *Reductions.* Now, reductions by primary invariants enable to conclude (cf. Section 5.3). Let $\mathfrak{p}_4, \mathfrak{q}_4$ and \mathfrak{p}_8 (resp. denoted $\mathfrak{c}_{16}, \mathfrak{c}_{17}$ and \mathfrak{c}_{121} in Appendix A) be the invariants defined by Proposition 8: they are the first three generators of a h.s.o.p of degrees 4, 4, 8, 12, 14, 16, 30 for $\mathbf{Inv}(S_9)$. So, instead of $\mathbf{Cov}_{d,m}(S_9)$, consider the quotient

$$\mathcal{Q}_{d,m} := \mathbf{Cov}_{d,m}(S_9) / (\mathfrak{p}_4 \mathbf{Cov}_{d-4,m}(S_9) + \mathfrak{q}_4 \mathbf{Cov}_{d-4,m}(S_9) + \mathfrak{p}_8 \mathbf{Cov}_{d-8,m}(S_9)).$$

Note that working in $\mathcal{Q}_{d,m}$ amounts to evaluate covariants at random forms \mathfrak{f} that zeroify $\mathfrak{p}_4, \mathfrak{q}_4$ and \mathfrak{p}_8 at Step (2) of Algorithm 2. Furthermore, we can derive from Equation (2.5) the relation

$$\dim \mathcal{Q}_{d,m} = \dim \mathbf{Cov}_{d,m}(S_9) - 2 \dim \mathbf{Cov}_{d-4,m}(S_9) + 2 \dim \mathbf{Cov}_{d-12,m}(S_9) - \dim \mathbf{Cov}_{d-16,m}(S_9). \quad (6.2)$$

Typically, we find $\dim \mathcal{Q}_{60,14} = 33\,360$, which is finally affordable with Algorithm 2.

6.1.6. *Linear algebra.* Finally, we are left with 633 spaces $\mathcal{Q}_{d,m}$, the dimension of which must be checked versus what is predicted by Equation (6.2). These dimensions go from 1 for $\mathcal{Q}_{1,9}$ to 33 360 for $\mathcal{Q}_{60,14}$. We did it modulo $p = 65521$. The whole computation took less than one day on a DELL computer with 32 processors (1400MHz AMD OPTERON). For instance, for $\mathcal{Q}_{60,14}$, it took three hours on one processor: two hours to compute the matrix M^\top in Step (3) of Algorithm 2 (its rank was 33 359) and one extra hour to find the missing generator in Step (4).

6.2. **Covariant basis of binary decimics.** As for $\mathbf{Cov}(S_9)$, a (possibly incomplete) minimal basis for $\mathbf{Cov}(S_{10})$ have been already computed in the past (see [13]). With our implementation of Olver's algorithm, we retrieve a basis with 510 generators. A complete but somehow unappealing definition for these generators is in Appendix B. We gather in Table 4 the number of generators for each degree and each order too.

d/o	0	2	4	6	8	10	12	14	16	18	20	22	24	26	#	Cum
1	—	—	—	—	—	1	—	—	—	—	—	—	—	—	1	1
2	1	—	1	—	1	—	1	—	1	—	—	—	—	—	5	6
3	—	1	—	2	1	1	2	1	1	1	1	—	1	—	12	18
4	1	—	3	1	3	3	2	3	1	2	1	1	—	1	22	40
5	—	3	3	4	5	4	5	2	4	—	2	—	—	—	32	72
6	4	2	5	8	6	8	2	4	—	1	—	—	—	—	40	112
7	—	7	10	8	12	2	4	—	1	—	—	—	—	—	44	156
8	5	8	11	15	4	7	—	1	—	—	—	—	—	—	51	207
9	5	13	19	8	7	—	1	—	—	—	—	—	—	—	53	260
10	8	20	13	13	—	1	—	—	—	—	—	—	—	—	55	315
11	8	18	21	—	1	—	—	—	—	—	—	—	—	—	48	363
12	12	30	1	2	—	—	—	—	—	—	—	—	—	—	45	408
13	15	16	2	—	—	—	—	—	—	—	—	—	—	—	33	441
14	13	17	—	—	—	—	—	—	—	—	—	—	—	—	30	471
15	19	—	1	—	—	—	—	—	—	—	—	—	—	—	20	491
16	5	3	—	—	—	—	—	—	—	—	—	—	—	—	8	499
17	5	—	—	—	—	—	—	—	—	—	—	—	—	—	5	504
18	1	1	—	—	—	—	—	—	—	—	—	—	—	—	2	506
19	2	—	—	—	—	—	—	—	—	—	—	—	—	—	2	508
20	—	—	—	—	—	—	—	—	—	—	—	—	—	—	—	508
21	2	—	—	—	—	—	—	—	—	—	—	—	—	—	2	510
Tot	106	139	90	61	40	27	17	11	8	4	4	1	1	1	510	

TABLE 4. Minimal basis of $\mathbf{Cov}(S_{10})$

The calculations that we have made to prove that this table is indeed complete are finally very similar to the ones for $\mathbf{Cov}(S_9)$. The main difficulty is again the computation of A_3 , especially we have to deal with $69 - 9 = 60$ covariants for $\mathbf{Cov}(S_8)$, of order 2, 4, 6, 8, 10, 12, 14, 18 (instead of the 21 covariants of $\mathbf{Cov}(S_6)$). The integer system (\mathcal{S}) is

$$(\mathcal{S}) \begin{cases} 10a_1 + 12a_2 + 16a_3 + 18a_4 + 20a_5 + 24a_6 + 26a_7 & = u + r, \\ 2(b_1 + \dots + b_{14}) + 4(b_{15} + \dots + b_{27}) + 6(b_{28} + \dots + b_{39}) + 8(b_{40} + \dots + b_{45}) + \\ 10(b_{46} + \dots + b_{52}) + 12(b_{53} + b_{54} + b_{55}) + 14(b_{56} + b_{57} + b_{58}) + 18(b_{59} + b_{60}) & = v + r. \end{cases}$$

It took here slightly less than 3 minutes on a laptop to find the 8985 minimal solutions of the injective companion $(\tilde{\mathcal{S}})$ of (\mathcal{S}) , which in return yields 1 345 290 951 minimal solutions for (\mathcal{S}) .

Relations and degree/order upper-bounds that we have for $\mathbf{Cov}(S_{10})$ improve a lot the situation. Especially, the order can not be larger than $\lambda_{10} = 26$ (see Lemma 2) and the degree upper-bounds for medium size orders are slightly better than the ones of $\mathbf{Cov}(S_9)$ (cf. Lemma 12).

So, we finally arrive at 588 spaces $\mathbf{Cov}_{d,m}(S_{10})$ to be checked. The largest one is $\mathbf{Cov}_{46,20}(S_{10})$, which is only of dimension 26323 if we work modulo the invariants $\mathfrak{p}'_2, \mathfrak{p}'_4, \mathfrak{p}'_6, \mathfrak{q}'_6$ (resp. denoted $\mathfrak{c}_2, \mathfrak{c}_{19}, \mathfrak{c}_{73}$ and \mathfrak{c}_{74} in Appendix B) of degree 2, 4, 6 and 6 defined in the h.s.o.p. of $\mathbf{Inv}(S_{10})$ [14] (cf. Proposition 9).

The whole computation was finally slightly easier than $\mathbf{Cov}(S_9)$, it took about 4 hours on the same DELL computer. All in all, we have proved this theorem.

Theorem 25. *The 510 covariants given in Appendix B define a minimal basis for the covariant algebra $\mathbf{Cov}(S_{10})$.*

ACKNOWLEDGEMENT

We would like to thank Hanspeter Kraft for pointing out the work of Michel Van den Bergh to us. We wish to express our grateful acknowledgment to Boris Kolev and Christophe Ritzentahler for fruitful discussions on preliminary versions of the paper too.

REFERENCES

- [1] A. Abdesselam. On the volume conjecture for classical spin networks. *J. Knot Theory Ramifications*, 21(3):1250022, 62, 2012.
- [2] A. Abdesselam and J. Chipalkatti. Brill-Gordan loci, transvectants and an analogue of the Foulkes conjecture. *Adv. Math.*, 208(2):491–520, 2007.
- [3] A. Abdesselam and J. Chipalkatti. The higher transvectants are redundant. *Ann. Inst. Fourier (Grenoble)*, 59(5):1671–1713, 2009.
- [4] A. Abdesselam and J. Chipalkatti. Quadratic involutions on binary forms. *Michigan Math. J.*, 61(2):279–296, 2012.
- [5] A. Adem and R. J. Milgram. *Cohomology of finite groups*, volume 309. Springer Science & Business Media, 2004.
- [6] L. Bedratyuk. On complete system of covariants for the binary form of degree 8. *Mat. Visn. Nauk. Tov. Im. Shevchenka*, 5:11–22, 2008.
- [7] L. Bedratyuk. A complete minimal system of covariants for the binary form of degree 7. *J. Symbolic Comput.*, 44(2):211–220, 2009.
- [8] L. Bedratyuk. The MAPLE package for calculating Poincaré series. *Journal of Symbolic Computation*, 2, 2011.
- [9] J.-P. Boehler. *Application of tensor functions in solid mechanics*. CISM Courses and Lectures. Springer-Verlag, Wien, 1987.
- [10] J.-P. Boehler, A. A. Kirillov, Jr., and E. T. Onat. On the polynomial invariants of the elasticity tensor. *J. Elasticity*, 34(2):97–110, 1994.
- [11] G. Boole. Exposition of a general theory of linear transformation. *Camb. Math.*, 3:1–20, 1841.
- [12] A. Brini, F. Regonati, and A. Teolis. Combinatorics, transvectants and superalgebras. An elementary constructive approach to Hilbert’s finiteness theorem. *Adv. in Appl. Math.*, 37(3):287–308, 2006.
- [13] A. E. Brouwer. Invariants of binary forms, 2015. Available at <http://www.win.tue.nl/~aeb/math/invar.html>.
- [14] A. E. Brouwer and M. Popoviciu. The invariants of the binary decimic. *J. Symbolic Comput.*, 45(8):837–843, 2010.
- [15] A. E. Brouwer and M. Popoviciu. The invariants of the binary nonic. *J. Symbolic Comput.*, 45(6):709–720, 2010.
- [16] A. E. Brouwer and M. Popoviciu. SL_2 -modules of small homological dimension. *Transform. Groups*, 16(3):599–617, 2011.
- [17] A. E. Brouwer and M. Popoviciu. Sylvester versus Gundelfinger. *SIGMA Symmetry Integrability Geom. Methods Appl.*, 8:Paper 075, 7, 2012.
- [18] W. Bruns and H. J. Herzog. *Cohen-macaulay rings*. Cambridge University Press, 1998.
- [19] W. Bruns, B. Ichim, T. Römer, and C. Söger. Normaliz 2.12. Technical report, Universität Osnabrück, 2015.
- [20] A. Cayley. A seventh memoir on quantics. *Philosophical Transactions of the Royal Society of London*, 151:277–292, 1861.
- [21] A. Cayley. *The collected mathematical papers. Volume 1-12*. Cambridge Library Collection. Cambridge University Press, Cambridge, 2009. Index, Reprint of the 1898 original.
- [22] M. Clausen and A. Fortenbacher. Efficient solution of linear Diophantine equations [MR1014196 (90i:11151)]. In *Unification*, pages 377–392. Academic Press, London, 1990.
- [23] A. Clebsch and P. Gordan. *Theorie der Abelschen Functionen*. Physica-Verlag, Würzburg, 1967. Thesaurus Mathematicae, (Neudrucke wichtiger mathematischer Werke), Band 7.
- [24] E. Contejean and H. Devie. Résolution de systèmes linéaires d’équations diophantiennes. *C. R. Acad. Sci. Paris Sér. I Math.*, 313(2):115–120, 1991.
- [25] T. Crilly. The rise of Cayley’s invariant theory (1841–1862). *Historia Math.*, 13(3):241–254, 1986.
- [26] T. Crilly. The decline of Cayley’s invariant theory (1863–1895). *Historia Math.*, 15(4):332–347, 1988.
- [27] H. L. Cröni. *Zur Berechnung von Kovarianten von Quantiken*. PhD thesis, Saarbrücken, Univ., 2002.
- [28] H. Derksen. Computation of invariants for reductive groups. *Adv. Math.*, 141(2):366–384, 1999.
- [29] H. Derksen and G. Kemper. *Computational invariant theory*. Invariant Theory and Algebraic Transformation Groups, I. Springer-Verlag, Berlin, 2002. Encyclopaedia of Mathematical Sciences, 130.
- [30] H. Derksen and G. Kemper. Computing invariants of algebraic groups in arbitrary characteristic. *Adv. Math.*, 217(5):2089–2129, 2008.
- [31] J. A. Dieudonné and J. B. Carrell. Invariant theory, old and new. *Advances in Math.*, 4:1–80 (1970), 1970.
- [32] J. Dixmier. Sur les invariants des formes binaires. *C. R. Acad. Sci. Paris Sér. I Math.*, 292(23):987–990, 1981.
- [33] J. Dixmier. Série de Poincaré et systèmes de paramètres pour les invariants des formes binaires de degré 7. *Bull. Soc. Math. France*, 110(3):303–318, 1982.
- [34] J. Dixmier. Quelques résultats et conjectures concernant les séries de Poincaré des invariants des formes binaires. In *Séminaire d’algèbre Paul Dubreil et Marie-Paule Malliavin, 36ème année (Paris, 1983–1984)*, volume 1146 of *Lecture Notes in Math.*, pages 127–160. Springer, Berlin, 1985.

- [35] J. Dixmier. Quelques résultats de finitude en théorie des invariants. *Astérisque*, 145-146:163–175, 1987. Séminaire Bourbaki, Vol. 1985/86.
- [36] J. Dixmier and D. Lazard. Le nombre minimum d’invariants fondamentaux pour les formes binaires de degré 7. *Portugal. Math.*, 43(3):377–392, 1985/86.
- [37] D. Eisenbud. *Commutative algebra, with a view toward algebraic geometry*. Springer, 1995.
- [38] J.-C. Faugère, P. Gaudry, L. Huot, and G. Renault. Using symmetries in the index calculus for elliptic curves discrete logarithm. *J. Cryptology*, 27(4):595–635, 2014.
- [39] J.-C. Faugère and J. Svartz. Solving polynomial systems globally invariant under an action of the symmetric group and application to the equilibria of n vortices in the plane. In *Proceedings of the 37th International Symposium on Symbolic and Algebraic Computation*, pages 170–178. ACM, 2012.
- [40] J.-C. Faugère and J. Svartz. Gröbner bases of ideals invariant under a commutative group: the non-modular case. In *Proceedings of the 38th international symposium on International symposium on symbolic and algebraic computation*, pages 347–354. ACM, 2013.
- [41] C. S. Fisher. The death of a mathematical theory. A study in the sociology of knowledge. *Arch. History Exact Sci.*, 3:137–159 (1966), 1966.
- [42] K. Geissler and J. Klüners. Galois group computation for rational polynomials. *Journal of Symbolic Computation*, 30(6):653–674, 2000.
- [43] P. Gordan. Beweis, dass jede Covariante und Invariante einer Binären Form eine ganze Function mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *Journal für die reine und angewandte Mathematik*, 1868.
- [44] P. Gordan. *Über das Formensystem Binärer Formen*. 1875.
- [45] P. Gordan. Die Hessische und die Cayley’sche Curve. *Trans. Amer. Math. Soc.*, 1(4):402–413, 1900.
- [46] P. Gordan. Formentheoretische Entwicklung der in Herrn White’s Abhandlung über Curven dritter Ordnung enthaltenen Sätze. *Trans. Amer. Math. Soc.*, 1(1):9–13, 1900.
- [47] P. Gordan. *Vorlesungen über Invariantentheorie*. Chelsea Publishing Co., New York, second edition, 1987. Erster Band: Determinanten. [Vol. I: Determinants], Zweiter Band: Binäre Formen. [Vol. II: Binary forms], Edited by Georg Kerschensteiner.
- [48] J. H. Grace and A. Young. *The algebra of invariants*. Cambridge Library Collection. Cambridge University Press, Cambridge, 2010. Reprint of the 1903 original.
- [49] A. Hashemi. Efficient Algorithms for Computing Noether Normalization. *Lecture Notes in Computer Science*, 5081:97–107, 2008.
- [50] R. Hemmecke, R. Hemmecke, M. Koeppe, P. Malkin, and M. Walter. 4ti2—a software package for algebraic, geometric and combinatorial problems on linear spaces. Available at <http://www.4ti2.de/>.
- [51] D. Hilbert. *Theory of algebraic invariants*. Cambridge University Press, Cambridge, 1993. Translated from the German and with a preface by Reinhard C. Laubenbacher, Edited and with an introduction by Bernd Sturmfels.
- [52] M. Hochster and J. L. Roberts. Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay. *Advances in Math.*, 13:115–175, 1974.
- [53] R. Howe. Remarks on classical invariant theory. *Trans. Amer. Math. Soc.*, 313(2):539–570, 1989.
- [54] R. Howe. Transcending classical invariant theory. *J. Amer. Math. Soc.*, 2(3):535–552, 1989.
- [55] G. Kemper. Computing invariants of reductive groups in positive characteristic. *Transform. Groups*, 8(2):159–176, 2003.
- [56] A. W. Knap. *Advanced algebra*. Cornerstones. Birkhäuser Boston, Inc., Boston, MA, 2007. Along with a companion volume it Basic algebra.
- [57] J. P. S. Kung and G.-C. Rota. The invariant theory of binary forms. *Bull. Amer. Math. Soc. (N.S.)*, 10(1):27–85, 1984.
- [58] S. Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.
- [59] R. Lercier and C. Ritzenhaller. Hyperelliptic curves and their invariants: geometric, arithmetic and algorithmic aspects. *J. Algebra*, 372:595–636, 2012.
- [60] P. Littelmann and C. Procesi. On the Poincaré series of the invariants of binary forms. *J. Algebra*, 133(2):490–499, 1990.
- [61] J.-G. Luque. *Invariants of hypermatrices*. Habilitation à diriger des recherches, Université de Marne la Vallée, Dec. 2008.
- [62] M. Olive. About Gordan’s algorithm for binary forms. *ArXiv e-prints*, Mar. 2014.
- [63] M. Olive. *Géométrie des espaces de tenseurs, une approche effective appliquée à la mécanique des milieux continus*. PhD thesis, Aix-Marseille University, 2014.
- [64] P. J. Olver. *Classical invariant theory*, volume 44 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1999.
- [65] K. H. Parshall. Toward a history of nineteenth-century invariant theory. In *The history of modern mathematics, Vol. I (Poughkeepsie, NY, 1989)*, pages 157–206. Academic Press, Boston, MA, 1989.
- [66] D. V. Pasechnik. Computing covariants of binary forms and related topics. *preprint*, 1996.

- [67] P. Pisón-Casares and A. Vigneron-Tenorio. N-solutions to linear systems over \mathbb{Z} . *Linear Algebra Appl.*, 384:135–154, 2004.
- [68] M. I. Popoviciu Draisma. *Invariants of binary forms*. PhD thesis, University of Basel, 2014.
- [69] R. Rivlin and J. Ericksen. Stress-deformation relations for isotropic materials. *J. Rational Mech. Anal.*, 4:323–425, 1955.
- [70] G. Smith and R. Rivlin. The strain-energy function for anisotropic elastic materials. *Trans. Amer. Math. Soc.*, 88:175–193, 1971.
- [71] T. A. Springer. Séries de Poincaré dans la théorie des invariants. In *Paul Dubreil and Marie-Paule Malliavin algebra seminar, 35th year (Paris, 1982)*, volume 1029 of *Lecture Notes in Math.*, pages 37–54. Springer, Berlin, 1983.
- [72] R. P. Stanley. Combinatorics and invariant theory. In *Relations between combinatorics and other parts of mathematics (Proc. Sympos. Pure Math., Ohio State Univ., Columbus, Ohio, 1978)*, Proc. Sympos. Pure Math., XXXIV, pages 345–355. Amer. Math. Soc., Providence, R.I., 1979.
- [73] R. P. Stanley. Invariants of finite groups and their applications to combinatorics. *Bulletin of the American Mathematical Society*, 1(3):475–511, 1979.
- [74] R. P. Stanley. *Combinatorics and commutative algebra*, volume 41 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, 1983.
- [75] R. P. Stanley. *Enumerative combinatorics. Volume 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, second edition, 2012.
- [76] R. P. Stauduhar. The determination of galois groups. *Mathematics of computation*, 27(124):981–996, 1973.
- [77] B. Sturmfels. *Algorithms in invariant theory*. Texts and Monographs in Symbolic Computation. Springer-WienNewYork, Vienna, second edition, 2008.
- [78] J. J. Sylvester. On an Application of the New Atomic Theory to the Graphical Representation of the Invariants and Covariants of Binary Quantics, With Three Appendices, [Continued]. *Amer. J. Math.*, 1(2):105–125, 1878.
- [79] J. J. Sylvester and F. Franklin. Tables of the Generating Functions and Groundforms for the Binary Quantics of the First Ten Orders. *Amer. J. Math.*, 2(3):223–251, 1879.
- [80] M. Van den Bergh. Cohen-Macaulayness of modules of covariants. *Invent. Math.*, 106(2):389–409, 1991.
- [81] M. Van den Bergh. Modules of covariants. In *Proceedings of the International Congress of Mathematics, ICM*, volume 94, pages 352–362, 1994.
- [82] F. von Gall. Ueber das simultane Formensystem einer Form 2ter und 6ter Ordnung. *Jahresbericht über das Gymnasium zu Lengo*, 1874.
- [83] F. von Gall. Ueber das vollständige System einer binären Form achter Ordnung. *Math. Ann.*, 17(1):139–152, 1880.
- [84] F. von Gall. Das vollständige formensystem der binären form 7ter ordnung. *Math. Ann.*, (31):318–336., 1888.
- [85] H. Weyl. *The classical groups*. Princeton Landmarks in Mathematics. Princeton University Press, Princeton, NJ, 1997. Their invariants and representations, Fifteenth printing, Princeton Paperbacks.
- [86] J. Weyman. Gordan ideals in the theory of binary forms. *J. Algebra*, 161(2):370–391, 1993.
- [87] Y. Yoshino and H. Matsumura. *Maximal Cohen-Macaulay Modules over Cohen-Macaulay Rings*, volume 146. Cambridge University Press, 1990.

APPENDIX A. A MINIMAL BASIS FOR $\mathbf{Cov}(\mathbf{S}_9)$

Degree 1: Order 9: $c_1 = f$	$c_{11} = (c_5, f)_6$ Order 13: $c_{12} = (c_5, f)_5$ Order 15: $c_{13} = (c_5, f)_4$ Order 17: $c_{14} = (c_5, f)_3$ Order 21: $c_{15} = (c_5, f)_1$	$c_{25} = (c_{14}, f)_8$ $c_{26} = (c_{13}, f)_7$ Order 12: $c_{27} = (c_{15}, f)_9$ $c_{28} = (c_{14}, f)_7$ Order 14: $c_{29} = (c_{15}, f)_8$ $c_{30} = (c_{14}, f)_6$ Order 16: $c_{31} = (c_{15}, f)_7$ Order 18: $c_{32} = (c_{15}, f)_6$ Order 22: $c_{33} = (c_{15}, f)_4$	$c_{40} = (c_{28}, f)_8$ $c_{41} = (c_{26}, f)_7$ Order 7: $c_{42} = (c_{31}, f)_9$ $c_{43} = (c_{30}, f)_8$ $c_{44} = (c_{29}, f)_8$ $c_{45} = (c_{28}, f)_7$ Order 9: $c_{46} = (c_{32}, f)_9$ $c_{47} = (c_{31}, f)_8$ $c_{48} = (c_{30}, f)_7$ Order 11: $c_{49} = (c_{32}, f)_8$ $c_{50} = (c_{31}, f)_7$ $c_{51} = (c_{30}, f)_6$ $c_{52} = (c_{29}, f)_6$ Order 13: $c_{53} = (c_{33}, f)_9$ $c_{54} = (c_{32}, f)_7$ Order 15: $c_{55} = (c_{33}, f)_8$ $c_{56} = (c_{32}, f)_6$ $c_{57} = (c_{31}, f)_5$ Order 19:	$c_{58} = (c_{33}, f)_6$ Degree 6: Order 2: $c_{59} = (c_{52}, f)_9$ $c_{60} = (c_{51}, f)_9$ $c_{61} = (c_{50}, f)_9$ $c_{62} = (c_{49}, f)_9$ Order 4: $c_{63} = (c_{54}, f)_9$ $c_{64} = (c_{53}, f)_9$ $c_{65} = (c_{52}, f)_8$ $c_{66} = (c_{51}, f)_8$ Order 6: $c_{67} = (c_{57}, f)_9$ $c_{68} = (c_{56}, f)_9$ $c_{69} = (c_{55}, f)_9$ $c_{70} = (c_{54}, f)_8$ $c_{71} = (c_{52}, f)_7$ $c_{72} = (c_{51}, f)_7$ Order 8: $c_{73} = (c_{57}, f)_8$ $c_{74} = (c_{56}, f)_8$ $c_{75} = (c_{55}, f)_8$ $c_{76} = (c_{54}, f)_7$	$c_{77} = (c_{53}, f)_7$ $c_{78} = (c_{52}, f)_6$ Order 10: $c_{79} = (c_{58}, f)_9$ $c_{80} = (c_{57}, f)_7$ $c_{81} = (c_{56}, f)_7$ Order 12: $c_{82} = (c_{58}, f)_8$ $c_{83} = (c_{57}, f)_6$ $c_{84} = (c_{56}, f)_6$ $c_{85} = (c_{55}, f)_6$ Order 16: $c_{86} = (c_{58}, f)_6$
Degree 2: Order 2: $c_2 = (f, f)_8$ Order 6: $c_3 = (f, f)_6$ Order 10: $c_4 = (f, f)_4$ Order 14: $c_5 = (f, f)_2$	Degree 4: Order 0: $c_{16} = (c_2, c_2)_2$ $c_{17} = (c_3, c_3)_6$ Order 4: $c_{18} = (c_{12}, f)_9$ $c_{19} = (c_{11}, f)_8$ Order 6: $c_{20} = (c_{13}, f)_9$ $c_{21} = (c_{12}, f)_8$ Order 8: $c_{22} = (c_{14}, f)_9$ $c_{23} = (c_{13}, f)_8$ $c_{24} = (c_{12}, f)_7$ Order 10:	Degree 5: Order 1: $c_{34} = (c_{26}, f)_9$ Order 3: $c_{35} = (c_{28}, f)_9$ $c_{36} = (c_{27}, f)_9$ $c_{37} = (c_{26}, f)_8$ Order 5: $c_{38} = (c_{30}, f)_9$ $c_{39} = (c_{29}, f)_9$			Degree 7: Order 1: $c_{87} = (c_{81}, f)_9$ $c_{88} = (c_{80}, f)_9$ $c_{89} = (c_{79}, f)_9$ $c_{90} = (c_{78}, f)_8$ Order 3: $c_{91} = (c_{85}, f)_9$ $c_{92} = (c_{84}, f)_9$ $c_{93} = (c_{83}, f)_9$ $c_{94} = (c_{82}, f)_9$

$c_{95} = (c_{81}, f)_8$
 $c_{96} = (c_{80}, f)_8$
 $c_{97} = (c_{78}, f)_7$

Order 5:

$c_{98} = (c_{85}, f)_8$
 $c_{99} = (c_{84}, f)_8$
 $c_{100} = (c_{83}, f)_8$
 $c_{101} = (c_{82}, f)_8$
 $c_{102} = (c_{81}, f)_7$
 $c_{103} = (c_{80}, f)_7$
 $c_{104} = (c_{79}, f)_7$
 $c_{105} = (c_{78}, f)_6$

Order 7:

$c_{106} = (c_{86}, f)_9$
 $c_{107} = (c_{85}, f)_7$
 $c_{108} = (c_{84}, f)_7$
 $c_{109} = (c_{83}, f)_7$
 $c_{110} = (c_{82}, f)_7$
 $c_{111} = (c_{81}, f)_6$
 $c_{112} = (c_{80}, f)_6$

Order 9:

$c_{113} = (c_{86}, f)_8$
 $c_{114} = (c_{85}, f)_6$
 $c_{115} = (c_{84}, f)_6$
 $c_{116} = (c_{83}, f)_6$
 $c_{117} = (c_{82}, f)_6$
 $c_{118} = (c_{81}, f)_5$

Order 11:

$c_{119} = (c_{86}, f)_7$

Order 13:

$c_{120} = (c_{86}, f)_6$

Degree 8:

Order 0:

$c_{121} = (c_2^3, c_3)_6$
 $c_{122} = (c_{118}, f)_9$
 $c_{123} = (c_7 c_{19}, f)_9$
 $c_{124} = (c_7 c_{18}, f)_9$
 $c_{125} = (c_6 c_{21}, f)_9$

Order 2:

$c_{126} = (c_{119}, f)_9$
 $c_{127} = (c_{118}, f)_8$
 $c_{128} = (c_{117}, f)_8$
 $c_{129} = (c_{116}, f)_8$
 $c_{130} = (c_{115}, f)_8$
 $c_{131} = (c_{114}, f)_8$
 $c_{132} = (c_{113}, f)_8$
 $c_{133} = (c_{112}, f)_7$

Order 4:

$c_{134} = (c_{120}, f)_9$
 $c_{135} = (c_{119}, f)_8$
 $c_{136} = (c_{118}, f)_7$
 $c_{137} = (c_{117}, f)_7$
 $c_{138} = (c_{116}, f)_7$
 $c_{139} = (c_{115}, f)_7$
 $c_{140} = (c_{114}, f)_7$
 $c_{141} = (c_{112}, f)_6$
 $c_{142} = (c_{111}, f)_6$
 $c_{143} = (c_{110}, f)_6$

Order 6:

$c_{144} = (c_{120}, f)_8$
 $c_{145} = (c_{119}, f)_7$
 $c_{146} = (c_{118}, f)_6$
 $c_{147} = (c_{117}, f)_6$
 $c_{148} = (c_{116}, f)_6$
 $c_{149} = (c_{115}, f)_6$
 $c_{150} = (c_{114}, f)_6$
 $c_{151} = (c_{113}, f)_6$
 $c_{152} = (c_{112}, f)_5$
 $c_{153} = (c_{111}, f)_5$

Order 8:

$c_{154} = (c_{120}, f)_7$
 $c_{155} = (c_{119}, f)_6$
 $c_{156} = (c_{118}, f)_5$
 $c_{157} = (c_{117}, f)_5$

Order 10:

$c_{158} = (c_{120}, f)_6$
 $c_{159} = (c_{119}, f)_5$

Degree 9:

Order 1:

$c_{160} = (c_{159}, f)_9$
 $c_{161} = (c_{158}, f)_9$
 $c_{162} = (c_{157}, f)_8$
 $c_{163} = (c_{156}, f)_8$
 $c_{164} = (c_{19} c_{21}, f)_9$
 $c_{165} = (c_{19} c_{20}, f)_9$
 $c_{166} = (c_{19}^2, f)_8$
 $c_{167} = (c_{18} c_{21}, f)_9$
 $c_{168} = (c_{18} c_{20}, f)_9$

Order 3:

$c_{169} = (c_{159}, f)_8$
 $c_{170} = (c_{158}, f)_8$
 $c_{171} = (c_{157}, f)_7$
 $c_{172} = (c_{156}, f)_7$
 $c_{173} = (c_{155}, f)_7$
 $c_{174} = (c_{154}, f)_7$
 $c_{175} = (c_{153}, f)_6$
 $c_{176} = (c_{152}, f)_6$

$c_{177} = (c_{151}, f)_6$
 $c_{178} = (c_{150}, f)_6$
 $c_{179} = (c_{149}, f)_6$
 $c_{180} = (c_{148}, f)_6$
 $c_{181} = (c_{147}, f)_6$
 $c_{182} = (c_{146}, f)_6$

Order 5:

$c_{183} = (c_{159}, f)_7$
 $c_{184} = (c_{158}, f)_7$
 $c_{185} = (c_{157}, f)_6$
 $c_{186} = (c_{156}, f)_6$
 $c_{187} = (c_{155}, f)_6$
 $c_{188} = (c_{154}, f)_6$
 $c_{189} = (c_{153}, f)_5$
 $c_{190} = (c_{152}, f)_5$
 $c_{191} = (c_{151}, f)_5$
 $c_{192} = (c_{150}, f)_5$

Order 7:

$c_{193} = (c_{159}, f)_6$
 $c_{194} = (c_{158}, f)_6$
 $c_{195} = (c_{157}, f)_5$
 $c_{196} = (c_{156}, f)_5$
 $c_{197} = (c_{155}, f)_5$
 $c_{198} = (c_{154}, f)_5$
 $c_{199} = (c_{153}, f)_4$

Order 9:

$c_{200} = (c_{159}, f)_5$

Degree 10:

Order 0:

$c_{201} = (c_{200}, f)_9$
 $c_{202} = (c_{37} c_{21}, f)_9$
 $c_{203} = (c_{36} c_{21}, f)_9$
 $c_{204} = (c_{37} c_{20}, f)_9$
 $c_{205} = (c_{19} c_{41}, f)_9$

Order 2:

$c_{206} = (c_{200}, f)_8$
 $c_{207} = (c_{199}, f)_7$
 $c_{208} = (c_{198}, f)_7$
 $c_{209} = (c_{197}, f)_7$
 $c_{210} = (c_{196}, f)_7$
 $c_{211} = (c_{195}, f)_7$
 $c_{212} = (c_{194}, f)_7$
 $c_{213} = (c_{24} c_{37}, f)_9$
 $c_{214} = (c_{24} c_{36}, f)_9$
 $c_{215} = (c_{24} c_{35}, f)_9$
 $c_{216} = (c_{34} c_{24}, f)_8$
 $c_{217} = (c_{23} c_{37}, f)_9$
 $c_{218} = (c_{23} c_{36}, f)_9$
 $c_{219} = (c_{23} c_{35}, f)_9$
 $c_{220} = (c_{23} c_{34}, f)_8$

Order 4:

$c_{221} = (c_{200}, f)_7$

$c_{222} = (c_{199}, f)_6$
 $c_{223} = (c_{198}, f)_6$
 $c_{224} = (c_{197}, f)_6$
 $c_{225} = (c_{196}, f)_6$
 $c_{226} = (c_{195}, f)_6$
 $c_{227} = (c_{194}, f)_6$
 $c_{228} = (c_{193}, f)_6$
 $c_{229} = (c_{192}, f)_5$
 $c_{230} = (c_{191}, f)_5$
 $c_{231} = (c_{190}, f)_5$
 $c_{232} = (c_{189}, f)_5$
 $c_{233} = (c_{188}, f)_5$
 $c_{234} = (c_{187}, f)_5$
 $c_{235} = (c_{186}, f)_5$

Order 6:

$c_{236} = (c_{200}, f)_6$
 $c_{237} = (c_{199}, f)_5$
 $c_{238} = (c_{198}, f)_5$

Order 8:

$c_{239} = (c_{200}, f)_5$

Degree 11:

Order 1:

$c_{240} = (c_{239}, f)_8$
 $c_{241} = (c_{41}^2, f)_9$
 $c_{242} = (c_{40} c_{41}, f)_9$
 $c_{243} = (c_{40}^2, f)_9$
 $c_{244} = (c_{39} c_{41}, f)_9$
 $c_{245} = (c_{39} c_{40}, f)_9$
 $c_{246} = (c_{39}^2, f)_9$
 $c_{247} = (c_{38} c_{41}, f)_9$
 $c_{248} = (c_{38} c_{40}, f)_9$
 $c_{249} = (c_{38} c_{39}, f)_9$
 $c_{250} = (c_{38}^2, f)_9$
 $c_{251} = (c_{45} c_{37}, f)_9$
 $c_{252} = (c_{44} c_{37}, f)_9$
 $c_{253} = (c_{37} c_{43}, f)_9$
 $c_{254} = (c_{37} c_{42}, f)_9$
 $c_{255} = (c_{37} c_{41}, f)_8$
 $c_{256} = (c_{37} c_{40}, f)_8$

Order 3:

$c_{257} = (c_{239}, f)_7$
 $c_{258} = (c_{238}, f)_6$
 $c_{259} = (c_{237}, f)_6$
 $c_{260} = (c_{236}, f)_6$
 $c_{261} = (c_{45} c_{41}, f)_9$
 $c_{262} = (c_{44} c_{41}, f)_9$
 $c_{263} = (c_{41} c_{43}, f)_9$
 $c_{264} = (c_{41} c_{42}, f)_9$
 $c_{265} = (c_{41}^2, f)_8$
 $c_{266} = (c_{45} c_{40}, f)_9$
 $c_{267} = (c_{44} c_{40}, f)_9$
 $c_{268} = (c_{40} c_{43}, f)_9$
 $c_{269} = (c_{40} c_{42}, f)_9$
 $c_{270} = (c_{40} c_{41}, f)_8$
 $c_{271} = (c_{40}^2, f)_8$
 $c_{272} = (c_{45} c_{39}, f)_9$

Order 5:

$c_{273} = (c_{239}, f)_6$
 $c_{274} = (c_{238}, f)_5$
 $c_{275} = (c_{237}, f)_5$
 $c_{276} = (c_{236}, f)_5$
 $c_{277} = (c_{235}, f)_4$
 $c_{278} = (c_{234}, f)_4$
 $c_{279} = (c_{233}, f)_4$

Order 7:

$c_{280} = (c_{239}, f)_5$

Degree 12:

Order 0:

$c_{281} = (c_{45} c_{62}, f)_9$
 $c_{282} = (c_{45} c_{61}, f)_9$
 $c_{283} = (c_{45} c_{60}, f)_9$
 $c_{284} = (c_{45} c_{59}, f)_9$
 $c_{285} = (c_{44} c_{62}, f)_9$

$c_{286} = (c_{44} c_{61}, f)_9$
 $c_{287} = (c_{44} c_{60}, f)_9$
 $c_{288} = (c_{62} c_{43}, f)_9$
 $c_{289} = (c_{61} c_{43}, f)_9$
 $c_{290} = (c_{66} c_{41}, f)_9$
 $c_{291} = (c_{41} c_{65}, f)_9$
 $c_{292} = (c_{41} c_{64}, f)_9$
 $c_{293} = (c_{37} c_{72}, f)_9$
 $c_{294} = (c_{37} c_{71}, f)_9$

Order 2:

$c_{295} = (c_{280}, f)_7$
 $c_{296} = (c_{66} c_{45}, f)_9$
 $c_{297} = (c_{45} c_{65}, f)_9$
 $c_{298} = (c_{45} c_{64}, f)_9$
 $c_{299} = (c_{45} c_{63}, f)_9$
 $c_{300} = (c_{45} c_{62}, f)_8$
 $c_{301} = (c_{45} c_{61}, f)_8$
 $c_{302} = (c_{45} c_{60}, f)_8$
 $c_{303} = (c_{45} c_{59}, f)_8$
 $c_{304} = (c_{44} c_{66}, f)_9$
 $c_{305} = (c_{44} c_{65}, f)_9$
 $c_{306} = (c_{44} c_{64}, f)_9$
 $c_{307} = (c_{44} c_{63}, f)_9$
 $c_{308} = (c_{44} c_{62}, f)_8$
 $c_{309} = (c_{44} c_{61}, f)_8$
 $c_{310} = (c_{44} c_{60}, f)_8$
 $c_{311} = (c_{44} c_{59}, f)_8$
 $c_{312} = (c_{66} c_{43}, f)_9$
 $c_{313} = (c_{43} c_{65}, f)_9$
 $c_{314} = (c_{64} c_{43}, f)_9$
 $c_{315} = (c_{63} c_{43}, f)_9$
 $c_{316} = (c_{62} c_{43}, f)_8$
 $c_{317} = (c_{61} c_{43}, f)_8$

Order 4:

$c_{318} = (c_{280}, f)_6$
 $c_{319} = (c_{279}, f)_5$
 $c_{320} = (c_{278}, f)_5$
 $c_{321} = (c_{277}, f)_5$

Order 6:

$c_{322} = (c_{280}, f)_5$

Degree 13:

Order 1:

$c_{323} = (c_{66} c_{72}, f)_9$
 $c_{324} = (c_{66} c_{71}, f)_9$
 $c_{325} = (c_{66} c_{70}, f)_9$
 $c_{326} = (c_{66} c_{69}, f)_9$
 $c_{327} = (c_{66} c_{68}, f)_9$
 $c_{328} = (c_{66} c_{67}, f)_9$
 $c_{329} = (c_{66}^2, f)_8$
 $c_{330} = (c_{72} c_{65}, f)_9$
 $c_{331} = (c_{71} c_{65}, f)_9$
 $c_{332} = (c_{70} c_{65}, f)_9$
 $c_{333} = (c_{69} c_{65}, f)_9$
 $c_{334} = (c_{68} c_{65}, f)_9$
 $c_{335} = (c_{67} c_{65}, f)_9$
 $c_{336} = (c_{66} c_{65}, f)_8$
 $c_{337} = (c_{65}^2, f)_8$
 $c_{338} = (c_{72} c_{64}, f)_9$
 $c_{339} = (c_{71} c_{64}, f)_9$
 $c_{340} = (c_{70} c_{64}, f)_9$
 $c_{341} = (c_{69} c_{64}, f)_9$
 $c_{342} = (c_{68} c_{64}, f)_9$
 $c_{343} = (c_{67} c_{64}, f)_9$
 $c_{344} = (c_{66} c_{64}, f)_8$
 $c_{345} = (c_{64} c_{65}, f)_8$
 $c_{346} = (c_{64}^2, f)_8$
 $c_{347} = (c_{72} c_{63}, f)_9$

Order 3:

$c_{348} = (c_{322}, f)_6$
 $c_{349} = (c_{72}^2, f)_9$
 $c_{350} = (c_{71} c_{72}, f)_9$
 $c_{351} = (c_{71}^2, f)_9$
 $c_{352} = (c_{70} c_{72}, f)_9$
 $c_{353} = (c_{70} c_{71}, f)_9$
 $c_{354} = (c_{70}^2, f)_9$

$c_{355} = (c_{69} c_{72}, f)_9$
 $c_{356} = (c_{69} c_{71}, f)_9$
 $c_{357} = (c_{69} c_{70}, f)_9$

Order 5:

$c_{358} = (c_{322}, f)_5$

Degree 14:

Order 0:

$c_{359} = (c_{78} c_{89}, f)_9$
 $c_{360} = (c_{88} c_{78}, f)_9$
 $c_{361} = (c_{78} c_{87}, f)_9$
 $c_{362} = (c_{77} c_{89}, f)_9$
 $c_{363} = (c_{77} c_{88}, f)_9$
 $c_{364} = (c_{89} c_{76}, f)_9$
 $c_{365} = (c_{72} c_{97}, f)_9$
 $c_{366} = (c_{72} c_{96}, f)_9$
 $c_{367} = (c_{72} c_{95}, f)_9$
 $c_{368} = (c_{72} c_{94}, f)_9$
 $c_{369} = (c_{93} c_{72}, f)_9$
 $c_{370} = (c_{92} c_{72}, f)_9$
 $c_{371} = (c_{91} c_{72}, f)_9$
 $c_{372} = (c_{71} c_{97}, f)_9$
 $c_{373} = (c_{71} c_{96}, f)_9$
 $c_{374} = (c_{71} c_{95}, f)_9$
 $c_{375} = (c_{112} c_{62}, f)_9$

Order 2:

$c_{376} = (c_{78} c_{97}, f)_9$
 $c_{377} = (c_{78} c_{96}, f)_9$
 $c_{378} = (c_{78} c_{95}, f)_9$
 $c_{379} = (c_{78} c_{94}, f)_9$
 $c_{380} = (c_{78} c_{93}, f)_9$
 $c_{381} = (c_{78} c_{92}, f)_9$
 $c_{382} = (c_{78} c_{91}, f)_9$
 $c_{383} = (c_{78} c_{90}, f)_8$
 $c_{384} = (c_{78} c_{89}, f)_8$
 $c_{385} = (c_{88} c_{78}, f)_8$
 $c_{386} = (c_{78} c_{87}, f)_8$
 $c_{387} = (c_{77} c_{97}, f)_9$
 $c_{388} = (c_{66} c_{112}, f)_9$

Order 4:

$c_{389} = (c_{358}, f)_5$

Degree 15:

Order 1:

$c_{390} = (c_{105}^2, f)_9$
 $c_{391} = (c_{104} c_{105}, f)_9$
 $c_{392} = (c_{104}^2, f)_9$
 $c_{393} = (c_{103} c_{105}, f)_9$
 $c_{394} = (c_{103} c_{104}, f)_9$
 $c_{395} = (c_{103}^2, f)_9$
 $c_{396} = (c_{102} c_{105}, f)_9$
 $c_{397} = (c_{102} c_{104}, f)_9$
 $c_{398} = (c_{102} c_{103}, f)_9$
 $c_{399} = (c_{102}^2, f)_9$
 $c_{400} = (c_{101} c_{105}, f)_9$
 $c_{401} = (c_{101} c_{104}, f)_9$
 $c_{402} = (c_{101} c_{103}, f)_9$
 $c_{403} = (c_{101} c_{102}, f)_9$
 $c_{404} = (c_{101}^2, f)_9$
 $c_{405} = (c_{100} c_{105}, f)_9$
 $c_{406} = (c_{100} c_{104}, f)_9$
 $c_{407} = (c_{100} c_{103}, f)_9$
 $c_{408} = (c_{100} c_{102}, f)_9$
 $c_{409} = (c_{100} c_{101}, f)_9$
 $c_{410} = (c_{100}^2, f)_9$
 $c_{411} = (c_{99} c_{105}, f)_9$
 $c_{412} = (c_{99} c_{104}, f)_9$
 $c_{413} = (c_{99} c_{103}, f)_9$
 $c_{414} = (c_{99} c_{102}, f)_9$
 $c_{415} = (c_{112} c_{97}, f)_9$

Order 3:

$c_{416} = (c_{112} c_{105}, f)_9$

Degree 16:

Order 0:

$c_{417} = (c_{133} c_{112}, f)_9$

$c_{418} = (c_{132} c_{112}, f)_9$

APPENDIX B. A MINIMAL BASIS FOR $\text{Cov}(S_{10})$

Degree 1: Order 10: $c_1 = f$	$c_{44} = (c_{34}, f)_{10}$ $c_{45} = (c_{33}, f)_{10}$ $c_{46} = (c_{32}, f)_{10}$ Order 6: $c_{47} = (c_{35}, f)_{10}$ $c_{48} = (c_{34}, f)_9$ $c_{49} = (c_{33}, f)_9$ $c_{50} = (c_{31}, f)_8$ Order 8: $c_{51} = (c_{37}, f)_{10}$ $c_{52} = (c_{36}, f)_{10}$ $c_{53} = (c_{35}, f)_9$ $c_{54} = (c_{34}, f)_8$ $c_{55} = (c_{33}, f)_8$ Order 10: $c_{56} = (c_{38}, f)_{10}$ $c_{57} = (c_{37}, f)_9$ $c_{58} = (c_{36}, f)_9$ $c_{59} = (c_{34}, f)_7$ Order 12: $c_{60} = (c_{39}, f)_{10}$ $c_{61} = (c_{38}, f)_9$ $c_{62} = (c_{37}, f)_8$ $c_{63} = (c_{36}, f)_8$ $c_{64} = (c_{34}, f)_6$ Order 14: $c_{65} = (c_{39}, f)_9$ $c_{66} = (c_{38}, f)_8$ Order 16: $c_{67} = (c_{40}, f)_{10}$ $c_{68} = (c_{39}, f)_8$ $c_{69} = (c_{38}, f)_7$ $c_{70} = (c_{37}, f)_6$ Order 18: $c_{71} = (c_{40}, f)_8$ $c_{72} = (c_{39}, f)_6$	$c_{109} = (c_{71}, f)_8$ $c_{110} = (c_{70}, f)_6$ $c_{111} = (c_{69}, f)_6$ Order 18: $c_{112} = (c_{72}, f)_6$ Degree 7: Order 2: $c_{113} = (c_{107}, f)_{10}$ $c_{114} = (c_{106}, f)_{10}$ $c_{115} = (c_{105}, f)_9$ $c_{116} = (c_{104}, f)_9$ $c_{117} = (c_{103}, f)_9$ $c_{118} = (c_{102}, f)_9$ $c_{119} = (c_{101}, f)_9$ Order 4: $c_{120} = (c_{111}, f)_{10}$ $c_{121} = (c_{110}, f)_{10}$ $c_{122} = (c_{109}, f)_{10}$ $c_{123} = (c_{108}, f)_{10}$ $c_{124} = (c_{107}, f)_9$ $c_{125} = (c_{106}, f)_9$ $c_{126} = (c_{105}, f)_8$ $c_{127} = (c_{104}, f)_8$ $c_{128} = (c_{103}, f)_8$ $c_{129} = (c_{102}, f)_8$ Order 6: $c_{130} = (c_{111}, f)_9$ $c_{131} = (c_{110}, f)_9$ $c_{132} = (c_{109}, f)_9$ $c_{133} = (c_{108}, f)_9$ $c_{134} = (c_{107}, f)_8$ $c_{135} = (c_{106}, f)_8$ $c_{136} = (c_{105}, f)_7$ $c_{137} = (c_{104}, f)_7$ Order 8: $c_{138} = (c_{112}, f)_{10}$ $c_{139} = (c_{111}, f)_8$ $c_{140} = (c_{110}, f)_8$ $c_{141} = (c_{109}, f)_8$ $c_{142} = (c_{108}, f)_8$ $c_{143} = (c_{107}, f)_7$ $c_{144} = (c_{106}, f)_7$ $c_{145} = (c_{105}, f)_6$ $c_{146} = (c_{104}, f)_6$ $c_{147} = (c_{103}, f)_6$ $c_{148} = (c_{102}, f)_6$ $c_{149} = (c_{101}, f)_6$ Order 10: $c_{150} = (c_{112}, f)_9$ $c_{151} = (c_{111}, f)_7$ Order 12: $c_{152} = (c_{112}, f)_8$ $c_{153} = (c_{111}, f)_6$ $c_{154} = (c_{110}, f)_6$ $c_{155} = (c_{109}, f)_6$ Order 16: $c_{156} = (c_{112}, f)_6$	$c_{176} = (c_{149}, f)_7$ $c_{177} = (c_{148}, f)_7$ $c_{178} = (c_{147}, f)_7$ $c_{179} = (c_{146}, f)_7$ $c_{180} = (c_{145}, f)_7$ Order 6: $c_{181} = (c_{156}, f)_{10}$ $c_{182} = (c_{155}, f)_8$ $c_{183} = (c_{154}, f)_8$ $c_{184} = (c_{153}, f)_8$ $c_{185} = (c_{152}, f)_8$ $c_{186} = (c_{151}, f)_7$ $c_{187} = (c_{150}, f)_7$ $c_{188} = (c_{149}, f)_6$ $c_{189} = (c_{148}, f)_6$ $c_{190} = (c_{147}, f)_6$ $c_{191} = (c_{146}, f)_6$ $c_{192} = (c_{145}, f)_6$ $c_{193} = (c_{144}, f)_6$ $c_{194} = (c_{143}, f)_6$ $c_{195} = (c_{142}, f)_6$ Order 8: $c_{196} = (c_{156}, f)_9$ $c_{197} = (c_{155}, f)_7$ $c_{198} = (c_{154}, f)_7$ $c_{199} = (c_{153}, f)_7$ Order 10: $c_{200} = (c_{156}, f)_8$ $c_{201} = (c_{155}, f)_6$ $c_{202} = (c_{154}, f)_6$ $c_{203} = (c_{153}, f)_6$ $c_{204} = (c_{152}, f)_6$ $c_{205} = (c_{151}, f)_5$ $c_{206} = (c_{150}, f)_5$ Order 14: $c_{207} = (c_{156}, f)_6$	$c_{248} = (c_{204}, f)_7$ $c_{249} = (c_{203}, f)_7$ $c_{250} = (c_{202}, f)_7$ $c_{251} = (c_{201}, f)_7$ $c_{252} = (c_{200}, f)_7$ Order 8: $c_{253} = (c_{207}, f)_8$ $c_{254} = (c_{206}, f)_6$ $c_{255} = (c_{205}, f)_6$ $c_{256} = (c_{204}, f)_6$ $c_{257} = (c_{203}, f)_6$ $c_{258} = (c_{202}, f)_6$ $c_{259} = (c_{201}, f)_6$ Order 12: $c_{260} = (c_{206}, f)_4$ Degree 10: Order 0: $c_{261} = (c_{26}c_{43}, f)_{10}$ $c_{262} = (c_{26}c_{42}, f)_{10}$ $c_{263} = (c_{26}c_{41}, f)_{10}$ $c_{264} = (c_{25}c_{43}, f)_{10}$ $c_{265} = (c_{25}c_{42}, f)_{10}$ $c_{266} = (c_{23}c_{46}, f)_{10}$ $c_{267} = (c_{23}c_{45}, f)_{10}$ $c_{268} = (c_{22}c_{50}, f)_{10}$ Order 2: $c_{269} = (c_{260}, f)_{10}$ $c_{270} = (c_{259}, f)_8$ $c_{271} = (c_{258}, f)_8$ $c_{272} = (c_{257}, f)_8$ $c_{273} = (c_{256}, f)_8$ $c_{274} = (c_{255}, f)_8$ $c_{275} = (c_{254}, f)_8$ $c_{276} = (c_{253}, f)_8$ $c_{277} = (c_{46}c_{26}, f)_{10}$ $c_{278} = (c_{45}c_{26}, f)_{10}$ $c_{279} = (c_{44}c_{26}, f)_{10}$ $c_{280} = (c_{26}c_{43}, f)_9$ $c_{281} = (c_{26}c_{42}, f)_9$ $c_{282} = (c_{26}c_{41}, f)_9$ $c_{283} = (c_{46}c_{25}, f)_{10}$ $c_{284} = (c_{45}c_{25}, f)_{10}$ $c_{285} = (c_{44}c_{25}, f)_{10}$ $c_{286} = (c_{25}c_{43}, f)_9$ $c_{287} = (c_{25}c_{42}, f)_9$ $c_{288} = (c_{25}c_{41}, f)_9$ Order 4: $c_{289} = (c_{260}, f)_9$ $c_{290} = (c_{259}, f)_7$ $c_{291} = (c_{258}, f)_7$ $c_{292} = (c_{257}, f)_7$ $c_{293} = (c_{256}, f)_7$ $c_{294} = (c_{255}, f)_7$ $c_{295} = (c_{254}, f)_7$ $c_{296} = (c_{253}, f)_7$ $c_{297} = (c_{252}, f)_6$ $c_{298} = (c_{251}, f)_6$ $c_{299} = (c_{250}, f)_6$ $c_{300} = (c_{249}, f)_6$ $c_{301} = (c_{248}, f)_6$ Order 6: $c_{302} = (c_{260}, f)_8$ $c_{303} = (c_{259}, f)_6$ $c_{304} = (c_{258}, f)_6$ $c_{305} = (c_{257}, f)_6$ $c_{306} = (c_{256}, f)_6$ $c_{307} = (c_{255}, f)_6$ $c_{308} = (c_{254}, f)_6$ $c_{309} = (c_{253}, f)_6$ $c_{310} = (c_{252}, f)_5$ $c_{311} = (c_{251}, f)_5$ $c_{312} = (c_{250}, f)_5$ $c_{313} = (c_{249}, f)_5$ $c_{314} = (c_{248}, f)_5$ Order 10: $c_{315} = (c_{260}, f)_6$	$c_{318} = (c_{46}c_{49}, f)_{10}$ $c_{319} = (c_{46}c_{48}, f)_{10}$ $c_{320} = (c_{46}c_{47}, f)_{10}$ $c_{321} = (c_{45}c_{50}, f)_{10}$ $c_{322} = (c_{45}c_{49}, f)_{10}$ $c_{323} = (c_{45}c_{48}, f)_{10}$ Order 2: $c_{324} = (c_{315}, f)_9$ $c_{325} = (c_{315}, f)_{10}$ $c_{326} = (c_{49}c_{50}, f)_{10}$ $c_{327} = (c_{49}, f)_{10}$ $c_{328} = (c_{48}c_{50}, f)_{10}$ $c_{329} = (c_{48}c_{49}, f)_{10}$ $c_{330} = (c_{48}, f)_{10}$ $c_{331} = (c_{47}c_{50}, f)_{10}$ $c_{332} = (c_{47}c_{49}, f)_{10}$ $c_{333} = (c_{47}c_{48}, f)_{10}$ $c_{334} = (c_{47}, f)_{10}$ $c_{335} = (c_{55}c_{46}, f)_{10}$ $c_{336} = (c_{46}c_{54}, f)_{10}$ $c_{337} = (c_{46}c_{53}, f)_{10}$ $c_{338} = (c_{46}c_{52}, f)_{10}$ $c_{339} = (c_{46}c_{51}, f)_{10}$ $c_{340} = (c_{46}c_{50}, f)_9$ $c_{341} = (c_{46}c_{49}, f)_9$ Order 4: $c_{342} = (c_{315}, f)_8$ $c_{343} = (c_{314}, f)_6$ $c_{344} = (c_{313}, f)_6$ $c_{345} = (c_{312}, f)_6$ $c_{346} = (c_{311}, f)_6$ $c_{347} = (c_{310}, f)_6$ $c_{348} = (c_{309}, f)_6$ $c_{349} = (c_{308}, f)_6$ $c_{350} = (c_{307}, f)_6$ $c_{351} = (c_{306}, f)_6$ $c_{352} = (c_{305}, f)_6$ $c_{353} = (c_{304}, f)_6$ $c_{354} = (c_{303}, f)_6$ $c_{355} = (c_{302}, f)_6$ $c_{356} = (c_{55}c_{50}, f)_{10}$ $c_{357} = (c_{50}c_{54}, f)_{10}$ $c_{358} = (c_{50}c_{53}, f)_{10}$ $c_{359} = (c_{50}c_{52}, f)_{10}$ $c_{360} = (c_{50}c_{51}, f)_{10}$ $c_{361} = (c_{50}, f)_9$ $c_{362} = (c_{55}c_{49}, f)_{10}$ Order 8: $c_{363} = (c_{315}, f)_6$ Degree 12: Order 0: $c_{364} = (c_{55}c_{78}, f)_{10}$ $c_{365} = (c_{55}c_{77}, f)_{10}$ $c_{366} = (c_{78}c_{54}, f)_{10}$ $c_{367} = (c_{50}c_{83}, f)_{10}$ $c_{368} = (c_{82}c_{50}, f)_{10}$ $c_{369} = (c_{81}c_{50}, f)_{10}$ $c_{370} = (c_{80}c_{50}, f)_{10}$ $c_{371} = (c_{79}c_{50}, f)_{10}$ $c_{372} = (c_{49}c_{83}, f)_{10}$ $c_{373} = (c_{49}c_{82}, f)_{10}$ $c_{374} = (c_{46}c_{91}, f)_{10}$ $c_{375} = (c_{46}c_{90}, f)_{10}$ Order 2: $c_{376} = (c_{363}, f)_8$ $c_{377} = (c_{55}c_{83}, f)_{10}$ $c_{378} = (c_{55}c_{82}, f)_{10}$ $c_{379} = (c_{55}c_{81}, f)_{10}$ $c_{380} = (c_{55}c_{80}, f)_{10}$ $c_{381} = (c_{55}c_{79}, f)_{10}$ $c_{382} = (c_{55}c_{78}, f)_9$ $c_{383} = (c_{55}c_{77}, f)_9$ $c_{384} = (c_{83}c_{54}, f)_{10}$ $c_{385} = (c_{82}c_{54}, f)_{10}$ $c_{386} = (c_{81}c_{54}, f)_{10}$ $c_{387} = (c_{80}c_{54}, f)_{10}$ $c_{388} = (c_{79}c_{54}, f)_{10}$ $c_{389} = (c_{78}c_{54}, f)_9$ $c_{390} = (c_{77}c_{54}, f)_9$ $c_{391} = (c_{83}c_{53}, f)_{10}$
---	---	---	---	---	--

$c_{392} = (c_{82}c_{53}, f)_{10}$	$c_{413} = (c_{83}c_{87}, f)_{10}$	$c_{437} = (c_{88}c_{87}, f)_{10}$	$c_{457} = (c_{127}c_{97}, f)_{10}$	$c_{480} = (c_{137}c_{128}, f)_{10}$	Degree 17:
$c_{393} = (c_{81}c_{53}, f)_{10}$	$c_{414} = (c_{83}c_{86}, f)_{10}$	$c_{438} = (c_{87}^2, f)_{10}$	$c_{458} = (c_{126}c_{97}, f)_{10}$	$c_{481} = (c_{136}c_{128}, f)_{10}$	Order 0:
$c_{394} = (c_{80}c_{53}, f)_{10}$	$c_{415} = (c_{83}c_{85}, f)_{10}$	$c_{439} = (c_{91}c_{86}, f)_{10}$	$c_{459} = (c_{125}c_{97}, f)_{10}$	$c_{482} = (c_{135}c_{128}, f)_{10}$	$c_{500} = (c_{180}c_{195}, f)_{10}$
$c_{395} = (c_{79}c_{53}, f)_{10}$	$c_{416} = (c_{83}c_{84}, f)_{10}$	Order 4:	$c_{460} = (c_{124}c_{97}, f)_{10}$	$c_{483} = (c_{134}c_{128}, f)_{10}$	$c_{501} = (c_{180}c_{194}, f)_{10}$
$c_{396} = (c_{78}c_{53}, f)_9$	$c_{417} = (c_{91}c_{82}, f)_{10}$	$c_{440} = (c_{408}, f)_6$	$c_{461} = (c_{123}c_{97}, f)_{10}$	$c_{484} = (c_{133}c_{128}, f)_{10}$	$c_{502} = (c_{180}c_{193}, f)_{10}$
$c_{397} = (c_{77}c_{53}, f)_9$	$c_{418} = (c_{90}c_{82}, f)_{10}$	$c_{441} = (c_{407}, f)_6$	$c_{462} = (c_{122}c_{97}, f)_{10}$	$c_{485} = (c_{132}c_{128}, f)_{10}$	$c_{503} = (c_{180}c_{192}, f)_{10}$
$c_{398} = (c_{83}c_{52}, f)_{10}$	$c_{419} = (c_{89}c_{82}, f)_{10}$	Degree 14:	$c_{463} = (c_{121}c_{97}, f)_{10}$	$c_{486} = (c_{128}c_{131}, f)_{10}$	$c_{504} = (c_{195}c_{175}, f)_{10}$
$c_{399} = (c_{82}c_{52}, f)_{10}$	$c_{420} = (c_{88}c_{82}, f)_{10}$	Order 0:	$c_{464} = (c_{97}c_{120}, f)_{10}$	$c_{487} = (c_{128}c_{130}, f)_{10}$	Degree 18:
$c_{400} = (c_{81}c_{52}, f)_{10}$	$c_{421} = (c_{82}c_{87}, f)_{10}$	$c_{442} = (c_{97}c_{119}, f)_{10}$	$c_{465} = (c_{97}c_{119}, f)_9$	$c_{488} = (c_{137}c_{127}, f)_{10}$	Order 0:
$c_{401} = (c_{80}c_{52}, f)_{10}$	$c_{422} = (c_{82}c_{86}, f)_{10}$	$c_{443} = (c_{118}c_{97}, f)_{10}$	$c_{466} = (c_{118}c_{97}, f)_9$	$c_{489} = (c_{136}c_{127}, f)_{10}$	$c_{505} = (c_{199}c_{225}, f)_{10}$
$c_{402} = (c_{79}c_{52}, f)_{10}$	$c_{423} = (c_{82}c_{85}, f)_{10}$	$c_{444} = (c_{117}c_{97}, f)_{10}$	$c_{467} = (c_{117}c_{97}, f)_9$	$c_{490} = (c_{135}c_{127}, f)_{10}$	Order 2:
$c_{403} = (c_{78}c_{52}, f)_9$	Order 2:	$c_{445} = (c_{116}c_{97}, f)_{10}$	$c_{468} = (c_{116}c_{97}, f)_9$	Order 4:	$c_{506} = (c_{195}c_{252}, f)_{10}$
$c_{404} = (c_{91}c_{50}, f)_{10}$	$c_{424} = (c_{91}^2, f)_{10}$	$c_{446} = (c_{115}c_{97}, f)_{10}$	$c_{469} = (c_{115}c_{97}, f)_9$	$c_{491} = (c_{137}c_{149}, f)_{10}$	Degree 16:
$c_{405} = (c_{90}c_{50}, f)_{10}$	$c_{425} = (c_{90}c_{91}, f)_{10}$	$c_{447} = (c_{114}c_{97}, f)_{10}$	$c_{470} = (c_{114}c_{97}, f)_9$	$c_{471} = (c_{113}c_{97}, f)_9$	Order 0:
Order 4:	$c_{426} = (c_{90}^2, f)_{10}$	$c_{448} = (c_{113}c_{97}, f)_{10}$	Degree 15:		$c_{492} = (c_{169}c_{149}, f)_{10}$
$c_{406} = (c_{363}, f)_7$	$c_{427} = (c_{89}c_{91}, f)_{10}$	$c_{449} = (c_{96}c_{119}, f)_{10}$	Order 0:		$c_{493} = (c_{168}c_{149}, f)_{10}$
Order 6:	$c_{428} = (c_{89}c_{90}, f)_{10}$	$c_{450} = (c_{96}c_{118}, f)_{10}$	$c_{472} = (c_{137}c_{129}, f)_{10}$		$c_{494} = (c_{167}c_{149}, f)_{10}$
$c_{407} = (c_{363}, f)_6$	$c_{429} = (c_{89}^2, f)_{10}$	$c_{451} = (c_{117}c_{96}, f)_{10}$	$c_{473} = (c_{136}c_{129}, f)_{10}$		$c_{495} = (c_{180}c_{137}, f)_{10}$
$c_{408} = (c_{362}, f)_4$	$c_{430} = (c_{88}c_{91}, f)_{10}$	$c_{452} = (c_{116}c_{96}, f)_{10}$	$c_{474} = (c_{135}c_{129}, f)_{10}$		$c_{496} = (c_{179}c_{137}, f)_{10}$
Degree 13:	$c_{431} = (c_{88}c_{90}, f)_{10}$	$c_{453} = (c_{115}c_{96}, f)_{10}$	$c_{475} = (c_{134}c_{129}, f)_{10}$		Order 2:
Order 0:	$c_{432} = (c_{88}c_{89}, f)_{10}$	$c_{454} = (c_{113}c_{96}, f)_{10}$	$c_{476} = (c_{133}c_{129}, f)_{10}$		$c_{497} = (c_{180}c_{149}, f)_{10}$
$c_{409} = (c_{91}c_{83}, f)_{10}$	$c_{433} = (c_{88}^2, f)_{10}$	Order 2:	$c_{477} = (c_{132}c_{129}, f)_{10}$		$c_{498} = (c_{179}c_{149}, f)_{10}$
$c_{410} = (c_{90}c_{83}, f)_{10}$	$c_{434} = (c_{91}c_{87}, f)_{10}$	$c_{455} = (c_{129}c_{97}, f)_{10}$	$c_{478} = (c_{129}c_{131}, f)_{10}$		$c_{499} = (c_{137}c_{195}, f)_{10}$
$c_{411} = (c_{89}c_{83}, f)_{10}$	$c_{435} = (c_{90}c_{87}, f)_{10}$	$c_{456} = (c_{128}c_{97}, f)_{10}$	$c_{479} = (c_{129}c_{130}, f)_{10}$		
$c_{412} = (c_{88}c_{83}, f)_{10}$	$c_{436} = (c_{89}c_{87}, f)_{10}$				

DGA MI, LA ROCHE MARGUERITE, 35174 BRUZ, FRANCE.

INSTITUT DE RECHERCHE MATHÉMATIQUE DE RENNES, UNIVERSITÉ DE RENNES 1, CAMPUS DE BEAULIEU, 35042 RENNES, FRANCE.

E-mail address: reynald.lercier@m4x.org

LMA, AIX-MARSEILLE UNIVERSITÉ, CENTRALE MARSEILLE, 13402 MARSEILLE CEDEX 20, FRANCE

E-mail address: marc.olive@math.cnrs.fr